

112TH CONGRESS  
1ST SESSION

# S. 1535

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

---

## IN THE SENATE OF THE UNITED STATES

SEPTEMBER 8, 2011

Mr. BLUMENTHAL introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

## A BILL

To protect consumers by mitigating the vulnerability of personally identifiable information to theft through a security breach, providing notice and remedies to consumers in the wake of such a breach, holding companies accountable for preventable breaches, facilitating the sharing of post-breach technical information between companies, and enhancing criminal and civil penalties and other protections against the unauthorized collection or use of personally identifiable information.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

2 (a) SHORT TITLE.—This Act may be cited as the  
 3 “Personal Data Protection and Breach Accountability Act  
 4 of 2011”.

5 (b) TABLE OF CONTENTS.—The table of contents of  
 6 this Act is as follows:

Sec. 1. Short title; table of contents.  
 Sec. 2. Findings.  
 Sec. 3. Definitions.

**TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND  
 OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY**

Sec. 101. Organized criminal activity in connection with unauthorized access to  
 personally identifiable information.  
 Sec. 102. Concealment of security breaches involving sensitive personally identi-  
 fiable information.  
 Sec. 103. Penalties for fraud and related activity in connection with computers.  
 Sec. 104. False notification.  
 Sec. 105. Unauthorized installation of personal information collection features  
 on a user’s computer.

**TITLE II—PRIVACY AND SECURITY OF PERSONALLY  
 IDENTIFIABLE INFORMATION**

**Subtitle A—A Data Privacy and Security Program**

Sec. 201. Purpose and applicability of data privacy and security program.  
 Sec. 202. Requirements for a personal data privacy and security program.  
 Sec. 203. Federal enforcement.  
 Sec. 204. Enforcement by State Attorneys General.  
 Sec. 205. Supplemental enforcement by individuals.

**Subtitle B—Security Breach Notification**

Sec. 211. Notice to individuals.  
 Sec. 212. Exemptions from notice to individuals.  
 Sec. 213. Methods of notice to individuals.  
 Sec. 214. Content of notice to individuals.  
 Sec. 215. Remedies for security breach.  
 Sec. 216. Notice to credit reporting agencies.  
 Sec. 217. Notice to law enforcement.  
 Sec. 218. Federal enforcement.  
 Sec. 219. Enforcement by State attorneys general.  
 Sec. 220. Supplemental enforcement by individuals.  
 Sec. 221. Relation to other laws.  
 Sec. 222. Authorization of appropriations.  
 Sec. 223. Reporting on risk assessment exemptions.

**Subtitle C—Post-Breach Technical Information Clearinghouse**

- Sec. 230. Clearinghouse information collection, maintenance, and access.  
 Sec. 231. Protections for clearinghouse participants.  
 Sec. 232. Effective date.

#### TITLE III—ACCESS TO AND USE OF COMMERCIAL DATA

- Sec. 301. General services administration review of contracts.  
 Sec. 302. Requirement to audit information security practices of contractors and third party business entities.  
 Sec. 303. Privacy impact assessment of government use of commercial information services containing personally identifiable information.  
 Sec. 304. FBI report on reported breaches and compliance.  
 Sec. 305. Department of Justice report on enforcement actions.  
 Sec. 306. Department of Justice report on enforcement actions.  
 Sec. 307. FBI report on notification effectiveness.

#### TITLE IV—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

- Sec. 401. Budget compliance.

### 1 **SEC. 2. FINDINGS.**

2 Congress finds that—

3 (1) databases of personally identifiable informa-  
 4 tion are increasingly prime targets of hackers, iden-  
 5 tity thieves, rogue employees, and other criminals,  
 6 including organized and sophisticated criminal oper-  
 7 ations;

8 (2) identity theft is a serious threat to the Na-  
 9 tion's economic stability, homeland security, the de-  
 10 velopment of e-commerce, and the privacy rights of  
 11 Americans;

12 (3) over 9,300,000 individuals were victims of  
 13 identity theft in America last year;

14 (4) security breaches are a serious threat to  
 15 consumer confidence, homeland security, e-com-  
 16 merce, and economic stability;

1           (5) it is important for business entities that  
2           own, use, or license personally identifiable informa-  
3           tion to adopt reasonable procedures to ensure the se-  
4           curity, privacy, and confidentiality of that personally  
5           identifiable information;

6           (6) individuals whose personal information has  
7           been compromised or who have been victims of iden-  
8           tity theft should receive the necessary information  
9           and assistance to mitigate their damages and to re-  
10          store the integrity of their personal information and  
11          identities;

12          (7) data brokers have assumed a significant  
13          role in providing identification, authentication, and  
14          screening services, and related data collection and  
15          analyses for commercial, nonprofit, and government  
16          operations;

17          (8) data misuse and use of inaccurate data have  
18          the potential to cause serious or irreparable harm to  
19          an individual's livelihood, privacy, and liberty and  
20          undermine efficient and effective business and gov-  
21          ernment operations;

22          (9) there is a need to ensure that data brokers  
23          conduct their operations in a manner that prioritizes  
24          fairness, transparency, accuracy, and respect for the  
25          privacy of consumers;

1           (10) government access to commercial data can  
2           potentially improve safety, law enforcement, and na-  
3           tional security;

4           (11) because government use of commercial  
5           data containing personal information potentially af-  
6           fects individual privacy, and law enforcement and  
7           national security operations, there is a need for Con-  
8           gress to exercise oversight over government use of  
9           commercial data;

10          (12) over 22,960,000 cases of data breaches in-  
11          volving personally identifiable information were re-  
12          ported through July of 2011, and in 2009 through  
13          2010, over 230,900,000 cases of personal data  
14          breaches were reported;

15          (13) facilitating information sharing among  
16          business entities and across sectors in the event of  
17          a breach can assist in remediating the breach and  
18          preventing similar breaches in the future;

19          (14) because the Federal Government has lim-  
20          ited resources, consumers themselves play a vital  
21          and complementary role in facilitating prompt notifi-  
22          cation and protecting against future breaches of se-  
23          curity;

24          (15) in addition to the immediate damages  
25          caused by security breaches, the lack of basic reme-

1 dial requirements often forces individuals whose sen-  
2 sitive personally identifiable information is com-  
3 promised as a result of a security breach to incur  
4 the economic costs of litigation to seek remedies, and  
5 the economic costs of fees required in many States  
6 to freeze compromised accounts; and

7 (16) victims of personal data breaches may suf-  
8 fer debilitating emotional and physical effects and  
9 become depressed or anxious, especially in cases of  
10 repeated or unresolved instances of data breaches.

11 **SEC. 3. DEFINITIONS.**

12 In this Act, the following definitions shall apply:

13 (1) **AFFILIATE.**—The term “affiliate” means  
14 persons related by common ownership or by cor-  
15 porate control.

16 (2) **AGENCY.**—The term “agency” has the  
17 meaning given such term in section 551 of title 5,  
18 United States Code.

19 (3) **BUSINESS ENTITY.**—The term “business  
20 entity” means any organization, corporation, trust,  
21 partnership, sole proprietorship, unincorporated as-  
22 sociation, or venture established to make a profit, or  
23 nonprofit.

24 (4) **CREDIT RATING AGENCY.**—The term “cred-  
25 it rating agency” has the meaning given such term

1 in section 3(a)(61) of the Securities Exchange Act  
2 of 1934 (12 U.S.C. 78c(a)(61)).

3 (5) CREDIT REPORT.—The term “credit report”  
4 means a consumer report, as that term is defined in  
5 section 603 of the Fair Credit Reporting Act (15  
6 U.S.C. 1681a).

7 (6) DATA BROKER.—The term “data broker”  
8 means a business entity which for monetary fees or  
9 dues regularly engages in the practice of collecting,  
10 transmitting, or providing access to sensitive person-  
11 ally identifiable information on more than 5,000 in-  
12 dividuals who are not the customers or employees of  
13 that business entity or affiliate primarily for the  
14 purposes of providing such information to non-  
15 affiliated third parties on an interstate basis.

16 (7) DATA FURNISHER.—The term “data fur-  
17 nisher” means any agency, organization, corpora-  
18 tion, trust, partnership, sole proprietorship, unincor-  
19 porated association, or nonprofit that serves as a  
20 source of information for a data broker.

21 (8) ENCRYPTION.—The term “encryption”—

22 (A) means the protection of data in elec-  
23 tronic form, in storage or in transit, using an  
24 encryption technology that has been adopted by  
25 a widely accepted standards setting body or,

1 has been widely accepted as an effective indus-  
2 try practice which renders such data indecipher-  
3 able in the absence of associated cryptographic  
4 keys necessary to enable decryption of such  
5 data; and

6 (B) includes appropriate management and  
7 safeguards of such cryptographic keys so as to  
8 protect the integrity of the encryption.

9 (9) IDENTITY THEFT.—The term “identity  
10 theft” means a violation of section 1028(a)(7) of  
11 title 18, United States Code.

12 (10) INTELLIGENCE COMMUNITY.—The term  
13 “intelligence community” includes the following:

14 (A) The Office of the Director of National  
15 Intelligence.

16 (B) The Central Intelligence Agency.

17 (C) The National Security Agency.

18 (D) The Defense Intelligence Agency.

19 (E) The National Geospatial-Intelligence  
20 Agency.

21 (F) The National Reconnaissance Office.

22 (G) Other offices within the Department of  
23 Defense for the collection of specialized national  
24 intelligence through reconnaissance programs.



1 (H) The intelligence elements of the Army,  
2 the Navy, the Air Force, the Marine Corps, the  
3 Federal Bureau of Investigation, and the De-  
4 partment of Energy.

5 (I) The Bureau of Intelligence and Re-  
6 search of the Department of State.

7 (J) The Office of Intelligence and Analysis  
8 of the Department of the Treasury.

9 (K) The elements of the Department of  
10 Homeland Security concerned with the analysis  
11 of intelligence information, including the Office  
12 of Intelligence of the Coast Guard.

13 (L) Such other elements of any other de-  
14 partment or agency as may be designated by  
15 the President, or designated jointly by the Di-  
16 rector of National Intelligence and the head of  
17 the department or agency concerned, as an ele-  
18 ment of the intelligence community.

19 (11) PERSONAL ELECTRONIC RECORD.—

20 (A) IN GENERAL.—The term “personal  
21 electronic record” means data associated with  
22 an individual contained in a database,  
23 networked or integrated databases, or other  
24 data system that is provided by a data broker  
25 to nonaffiliated third parties and includes per-

1           sonally identifiable information about that indi-  
2           vidual.

3           (B) EXCLUSIONS.—The term “personal  
4           electronic record” does not include—

5                   (i) any data related to an individual’s  
6                   past purchases of consumer goods; or

7                   (ii) any proprietary assessment or  
8                   evaluation of an individual or any propri-  
9                   etary assessment or evaluation of informa-  
10                  tion about an individual.

11           (12) PERSONALLY IDENTIFIABLE INFORMA-  
12           TION.—The term “personally identifiable informa-  
13           tion” means any information, or compilation of in-  
14           formation, in electronic or digital form that is a  
15           means of identification (as defined in section  
16           1028(d)(7) of title 18, United State Code).

17           (13) PREDISPUTE ARBITRATION AGREEMENT.—  
18           The term “predispute arbitration agreement” means  
19           any agreement to arbitrate a dispute that had not  
20           yet arisen at the time of the making of the agree-  
21           ment.

22           (14) PUBLIC RECORD SOURCE.—The term  
23           “public record source” means the Congress, any  
24           agency, any State or local government agency, the  
25           government of the District of Columbia and govern-

1       ments of the territories or possessions of the United  
2       States, and Federal, State or local courts, courts  
3       martial and military commissions, that maintain  
4       personally identifiable information in records avail-  
5       able to the public.

6               (15) SECURITY BREACH.—

7               (A) IN GENERAL.—The term “security  
8       breach” means compromise of the security, con-  
9       fidentiality, or integrity of computerized data  
10      through misrepresentation or actions—

11              (i) that result in, or that there is a  
12      reasonable basis to conclude has resulted  
13      in—

14              (I) the unauthorized acquisition  
15      of sensitive personally identifiable in-  
16      formation; or

17              (II) access to sensitive personally  
18      identifiable information that is for an  
19      unauthorized purpose, or in excess of  
20      authorization; and

21              (ii) which present a significant risk of  
22      harm or fraud to any individual.

23              (B) EXCLUSION.—The term “security  
24      breach” does not include—

1 (i) a good faith acquisition of sensitive  
2 personally identifiable information by a  
3 business entity or agency, or an employee  
4 or agent of a business entity or agency, if  
5 the sensitive personally identifiable infor-  
6 mation is not subject to further unauthor-  
7 ized disclosure;

8 (ii) the release of a public record not  
9 otherwise subject to confidentiality or non-  
10 disclosure requirements; or

11 (iii) any lawfully authorized criminal  
12 investigation or authorized investigative,  
13 protective, or intelligence activities that are  
14 carried out by or on behalf of any element  
15 of the intelligence community and con-  
16 ducted in accordance with the United  
17 States laws, authorities, and regulations  
18 governing such intelligence activities.

19 (16) SECURITY FREEZE.—The term “security  
20 freeze” means a notice, at the request of the con-  
21 sumer and subject to exceptions in section 215(b),  
22 that prohibits the consumer reporting agency from  
23 releasing all or any part of the consumer’s credit re-  
24 port or any information derived from it without the  
25 express authorization of the consumer.

1           (17) SENSITIVE PERSONALLY IDENTIFIABLE IN-  
 2           FORMATION.—The term “sensitive personally identi-  
 3           fiable information” means any information or com-  
 4           pilation of information, in electronic or digital form  
 5           that includes—

6                   (A) an individual’s first and last name or  
 7                   first initial and last name in combination with  
 8                   any 1 of the following data elements:

9                           (i) A nontruncated social security  
 10                           number, driver’s license number, passport  
 11                           number, or alien registration number.

12                           (ii) Any 2 of the following:

13                                   (I) Home address.

14                                   (II) Telephone number.

15                                   (III) Mother’s maiden name.

16                                   (IV) Month, day, and year of  
 17                                   birth.

18                           (iii) Unique biometric data such as a  
 19                           finger print, voice print, a retina or iris  
 20                           image, or any other unique physical rep-  
 21                           resentation.

22                           (iv) A unique account identifier, elec-  
 23                           tronic identification number, user name, or  
 24                           routing code in combination with any asso-  
 25                           ciated security code, access code, or pass-

1 word if the code or password is required  
2 for an individual to obtain money, goods,  
3 services, or any other thing of value;

4 (B) a financial account number or credit  
5 or debit card number in combination with any  
6 security code, access code, or password that is  
7 required for an individual to obtain credit, with-  
8 draw funds, or engage in a financial trans-  
9 action; or

10 (C) any other combination of data ele-  
11 ments that could allow unauthorized access to  
12 or acquisition of the information described in  
13 subparagraph (A) or (B), including—

- 14 (i) a unique account identifier;  
15 (ii) an electronic identification num-  
16 ber;  
17 (iii) a user name;  
18 (iv) a routing code; or  
19 (v) any associated security code, ac-  
20 cess code, or password or any associated  
21 security questions and answers that could  
22 allow unauthorized access to the account.

1 **TITLE I—ENHANCING PUNISH-**  
 2 **MENT FOR IDENTITY THEFT**  
 3 **AND OTHER VIOLATIONS OF**  
 4 **DATA PRIVACY AND SECU-**  
 5 **RITY**

6 **SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**  
 7 **WITH UNAUTHORIZED ACCESS TO PERSON-**  
 8 **ALLY IDENTIFIABLE INFORMATION.**

9 Section 1961(1) of title 18, United States Code, is  
 10 amended by inserting “section 1030 (relating to fraud and  
 11 related activity in connection with computers) if the act  
 12 is a felony,” before “section 1084”.

13 **SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLV-**  
 14 **ING SENSITIVE PERSONALLY IDENTIFIABLE**  
 15 **INFORMATION.**

16 (a) IN GENERAL.—Chapter 47 of title 18, United  
 17 States Code, is amended by adding at the end the fol-  
 18 lowing:

19 **“§ 1041. Concealment of security breaches involving**  
 20 **sensitive personally identifiable informa-**  
 21 **tion**

22 “(a) Whoever, having knowledge of a security breach  
 23 and having the obligation to provide notice of such breach  
 24 to individuals under the Personal Data Protection and  
 25 Breach Accountability Act of 2011, and having not other-

1 wise qualified for an exemption from providing notice  
 2 under section 212 of the Personal Data Protection and  
 3 Breach Accountability Act of 2011, intentionally or will-  
 4 fully conceals the fact of such security breach and which  
 5 breach causes economic damage or substantial emotional  
 6 distress to 1 or more persons, shall be fined under this  
 7 title or imprisoned not more than 5 years, or both.

8 “(b) For purposes of subsection (a), the term ‘person’  
 9 has the same meaning as in section 1030(e)(12) of title  
 10 18, United States Code.

11 “(c) Any person seeking an exemption under section  
 12 212(b) of the Personal Data Protection and Breach Ac-  
 13 countability Act of 2011 shall be immune from prosecution  
 14 under this section if the United States Secret Service does  
 15 not indicate, in writing, that such notice be given under  
 16 section 212(b)(3) of the Personal Data Protection and  
 17 Breach Accountability Act of 2011.”.

18 (b) CONFORMING AND TECHNICAL AMENDMENTS.—  
 19 The table of sections for chapter 47 of title 18, United  
 20 States Code, is amended by adding at the end the fol-  
 21 lowing:

“1041. Concealment of security breaches involving personally identifiable infor-  
 mation.”.

22 (c) ENFORCEMENT AUTHORITY.—



1           (1) IN GENERAL.—The United States Secret  
2           Service shall have the authority to investigate of-  
3           fenses under this section.

4           (2) NONEXCLUSIVITY.—The authority granted  
5           in paragraph (1) shall not be exclusive of any exist-  
6           ing authority held by any other Federal agency.

7   **SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY**  
8                           **IN CONNECTION WITH COMPUTERS.**

9           Section 1030(c) of title 18, United States Code, is  
10          amended—

11           (1) by inserting “or conspiracy” after “or an  
12           attempt” each place it appears, except for paragraph  
13           (4);

14           (2) in paragraph (2)(B)—

15                   (A) in clause (i), by inserting “, or attempt  
16                   or conspiracy or conspiracy to commit an of-  
17                   fense,” after “the offense”;

18                   (B) in clause (ii), by inserting “, or at-  
19                   tempt or conspiracy or conspiracy to commit an  
20                   offense,” after “the offense”; and

21                   (C) in clause (iii), by inserting “(or, in the  
22                   case of an attempted offense, would, if com-  
23                   pleted, have obtained)” after “information ob-  
24                   tained”; and

25           (3) in paragraph (4)—

1 (A) in subparagraph (A)—

2 (i) by striking clause (ii);

3 (ii) by striking “in the case of—” and  
 4 all that follows through “an offense under  
 5 subsection (a)(5)(B)” and inserting “in the  
 6 case of an offense, or an attempt or con-  
 7 spiracy to commit an offense, under sub-  
 8 section (a)(5)(B)”;

9 (iii) by inserting “or conspiracy” after  
 10 “if the offense”;

11 (iv) by redesignating subclauses (I)  
 12 through (VI) as clauses (i) through (vi),  
 13 respectively, and adjusting the margin ac-  
 14 cordingly; and

15 (v) in clause (vi), as so redesignated,  
 16 by striking “; or” and inserting a semi-  
 17 colon;

18 (B) in subparagraph (B)—

19 (i) by striking clause (ii);

20 (ii) by striking “in the case of—” and  
 21 all that follows through “an offense under  
 22 subsection (a)(5)(A)” and inserting “in the  
 23 case of an offense, or an attempt or con-  
 24 spiracy to commit an offense, under sub-  
 25 section (a)(5)(A)”;

1 (iii) by inserting “or conspiracy” after  
 2 “if the offense”; and

3 (iv) by striking “; or” and inserting a  
 4 semicolon;

5 (C) in subparagraph (C)—

6 (i) by striking clause (ii);

7 (ii) by striking “in the case of—” and  
 8 all that follows through “an offense or an  
 9 attempt to commit an offense” and insert-  
 10 ing “in the case of an offense, or an at-  
 11 tempt or conspiracy to commit an of-  
 12 fense,”; and

13 (iii) by striking “; or” and inserting a  
 14 semicolon;

15 (D) in subparagraph (D)—

16 (i) by striking clause (ii);

17 (ii) by striking “in the case of—” and  
 18 all that follows through “an offense or an  
 19 attempt to commit an offense” and insert-  
 20 ing “in the case of an offense, or an at-  
 21 tempt or conspiracy to commit an of-  
 22 fense,”; and

23 (iii) by striking “; or” and inserting a  
 24 semicolon;

1 (E) in subparagraph (E), by inserting “or  
2 conspires” after “offender attempts”;

3 (F) in subparagraph (F), by inserting “or  
4 conspires” after “offender attempts”; and

5 (G) in subparagraph (G)(ii), by inserting  
6 “or conspiracy” after “an attempt”.

7 **SEC. 104. FALSE NOTIFICATION.**

8 (a) IN GENERAL.—It shall be unlawful for an indi-  
9 vidual to send a notification of a breach of security that  
10 is false or intentionally misleading in order to obtain sen-  
11 sitive personally identifiable information in an effort to de-  
12 fraud an individual.

13 (b) PENALTY.—Any person that violates subsection  
14 (a) shall be fined not more than \$1,000,000, imprisoned  
15 not more than 5 years, or both.

16 (c) RULE OF CONSTRUCTION.—For purposes of this  
17 section, any single action or conduct that violates sub-  
18 section (a) with respect to multiple protected computers  
19 shall be construed to be a single violation.

20 **SEC. 105. UNAUTHORIZED INSTALLATION OF PERSONAL IN-**  
21 **FORMATION COLLECTION FEATURES ON A**  
22 **USER’S COMPUTER.**

23 (a) DEFINITION.—In this section, the term “pro-  
24 tected computer” has the meaning given the term in sec-  
25 tion 1030(e)(2) of title 18, United States Code.

1 (b) IN GENERAL.—It shall be unlawful for a person  
2 that is not an authorized user of a protected computer  
3 to cause the installation on the protected computer of soft-  
4 ware that collects sensitive personally identifiable informa-  
5 tion from an authorized user, unless the person—

6 (1) provides a clear and conspicuous disclosure  
7 of such collection; and

8 (2) obtains the consent of an authorized user of  
9 the protected computer prior to any collection of  
10 sensitive personally identifiable information.

11 (c) COLLECTION AND USE OF PERSONAL INFORMA-  
12 TION IN WEB SEARCHES.—It shall be unlawful for an  
13 Internet service provider or proxy server to knowingly or  
14 intentionally—

15 (1) bypass the display of search engine results  
16 and redirect web searches or queries entered by an  
17 authorized user of a protected computer directly to  
18 a commercial website, counterfeit web page, or tar-  
19 geted advertisement and derive an economic benefit  
20 from such activity; or

21 (2) monitor, manipulate, aggregate, and market  
22 the data collected in the process of intercepting a  
23 web search or query entered by an authorized user  
24 of a protected computer and derive an economic ben-  
25 efit from such activity.

1 (d) OTHER COLLECTION OF PERSONAL INFORMA-  
2 TION.—

3 (1) IN GENERAL.—It shall be unlawful for a  
4 person who is not an authorized user of a protected  
5 computer to cause the installation on the protected  
6 computer of software that engages in any of the col-  
7 lection practices described in paragraph (2), unless  
8 the person—

9 (A) provides a clear and conspicuous dis-  
10 closure of such collection; and

11 (B) obtains the consent of an authorized  
12 user of the protected computer prior to any  
13 such collection of information.

14 (2) COLLECTION PRACTICES DESCRIBED.—The  
15 collection practices described in this paragraph  
16 are—

17 (A) the use of a keystroke-logging function  
18 that records all or substantially all keystrokes  
19 made by an owner or operator of a computer  
20 and transfers that information from the com-  
21 puter to another person;

22 (B) the collection of data in a manner  
23 that—

24 (i) correlates sensitive personally iden-  
25 tifiable information with a history of—

1 (I) all, or substantially all, of the  
 2 websites visited by an owner or oper-  
 3 ator, other than websites operated by  
 4 the person providing such software; or

5 (II) all, or substantially all, of  
 6 the web searches conducted by an  
 7 owner or operator other than search  
 8 data collected by a search engine; and

9 (ii) uses the information described in  
 10 clause (i) to deliver advertising to, or dis-  
 11 play advertising on, the computer; and

12 (C) the extracting from the hard drive or  
 13 other storage medium of the computer—

14 (i) the substantive contents of files,  
 15 data, software, or other information know-  
 16 ingly saved or installed by the authorized  
 17 user of a protected computer; or

18 (ii) the substantive contents of com-  
 19 munications sent by an authorized user of  
 20 a protected computer to any other com-  
 21 puter.

22 (e) EXCEPTION.—This section shall not restrict a  
 23 person from causing the installation of software that col-  
 24 lects information for the provider of an online service or  
 25 website knowingly used or subscribed to by an authorized

1 user if the information collected is used only to affect the  
2 experience of the user while using that online service or  
3 website.

4 (f) UNINSTALL FUNCTIONALITY.—

5 (1) IN GENERAL.—Software that performs any  
6 function described in subsection (b) or (c) shall have  
7 the capability to subsequently be uninstalled or dis-  
8 abled by an authorized user through a program re-  
9 moval function that is usual and customary with the  
10 operating system of the computer or otherwise as  
11 clearly and conspicuously disclosed to the user.

12 (2) AUTHORITY TO UNINSTALL.—Software that  
13 enables an authorized user of a protected computer,  
14 such as a parent, employer, or system administrator,  
15 to choose to prevent another user of the same com-  
16 puter from uninstalling or disabling the software  
17 shall not be considered to prevent reasonable efforts  
18 to uninstall or disable the software within the mean-  
19 ing of paragraph (1) if not less than 1 authorized  
20 user retains the ability to uninstall or disable the  
21 software.

22 (g) LIMITATIONS ON LIABILITY.—

23 (1) IN GENERAL.—The restrictions imposed  
24 under this section do not apply to any monitoring of,  
25 or interaction with, a subscriber's Internet or other



1 network connection or service, or a protected com-  
2 puter, by or at the direction of a telecommunications  
3 carrier, cable operator, computer hardware or soft-  
4 ware provider, financial institution or provider of in-  
5 formation services or interactive computer service  
6 for—

7 (A) network or computer security pur-  
8 poses;

9 (B) diagnostics;

10 (C) technical support;

11 (D) repair;

12 (E) network management;

13 (F) authorized updates of software or sys-  
14 tem firmware;

15 (G) authorized remote system manage-  
16 ment;

17 (H) authorized provision of protection for  
18 users of the computer from objectionable con-  
19 tent;

20 (I) authorized scanning for computer soft-  
21 ware used in violation of this section for re-  
22 moval by an authorized user; or

23 (J) detection or prevention of the unau-  
24 thorized use of software fraudulent or other ille-  
25 gal activities.

1           (2) MANUFACTURER'S LIABILITY FOR THIRD-  
2       PARTY SOFTWARE.—A manufacturer or retailer of a  
3       computer shall not be liable under any provision of  
4       this section for causing the installation on the com-  
5       puter, prior to the first retail sale and delivery of the  
6       computer, of third-party branded software, unless  
7       the manufacturer or retailer knowingly allows the in-  
8       stallation of such third-party branded software and  
9       derives a benefit from the operation of such soft-  
10      ware.

11          (3) EXCEPTION FOR AUTHORIZED INVESTIGA-  
12      TIVE AGENCIES.—Nothing in this section prohibits  
13      any lawfully authorized criminal investigation or au-  
14      thorized investigative, protective, or intelligence ac-  
15      tivities that are carried out by or on behalf of any  
16      element of the intelligence community and conducted  
17      in accordance with the United States laws, authori-  
18      ties, and regulations governing such intelligence ac-  
19      tivities, of a law enforcement agency of the United  
20      States, a State, or a political subdivision of a State,  
21      or of an intelligence agency of the United States.

22      (h) ENFORCEMENT BY THE ATTORNEY GENERAL.—

23          (1) LIABILITY AND PENALTY FOR VIOLA-  
24      TIONS.—Any person who engages in an activity in  
25      violation of this section shall be fined not more than

1       \$500,000, imprisoned not more than 5 years, or  
2       both.

3               (2) ENHANCED LIABILITY AND PENALTIES FOR  
4       PATTERN OR PRACTICE OF VIOLATIONS.—

5               (A) IN GENERAL.—Any person who en-  
6       gages in a pattern or practice of activity that  
7       violates the provisions of this section shall be  
8       fined not more than \$1,000,000, imprisoned not  
9       more than 5 years, or both.

10              (B) TREATMENT OF SINGLE ACTION OR  
11       CONDUCT.—For purposes of subparagraph (A),  
12       any single action or conduct that violates this  
13       section with respect to multiple protected com-  
14       puters shall be construed as a single violation.

15              (3) CONSIDERATIONS.—In determining the  
16       amount of any penalty under paragraph (1) or (2),  
17       the court shall take into account—

18              (A) the degree of culpability of the defend-  
19       ant;

20              (B) any history of prior such conduct;

21              (C) the ability of the defendant to pay any  
22       fine imposed;

23              (D) the effect on the ability of the defend-  
24       ant to continue to do business; and

1 (E) such other matters as justice may re-  
 2 quire.

3 **TITLE II—PRIVACY AND SECU-**  
 4 **RITY OF PERSONALLY IDEN-**  
 5 **TIFIABLE INFORMATION**

6 **Subtitle A—A Data Privacy and**  
 7 **Security Program**

8 **SEC. 201. PURPOSE AND APPLICABILITY OF DATA PRIVACY**  
 9 **AND SECURITY PROGRAM.**

10 (a) PURPOSE.—The purpose of this subtitle is to en-  
 11 sure standards for developing and implementing adminis-  
 12 trative, technical, and physical safeguards to protect the  
 13 security of sensitive personally identifiable information.

14 (b) IN GENERAL.—A business entity engaging in  
 15 interstate commerce that involves collecting, accessing,  
 16 transmitting, using, storing, or disposing of sensitive per-  
 17 sonally identifiable information in electronic or digital  
 18 form on 10,000 or more United States persons is subject  
 19 to the requirements for a data privacy and security pro-  
 20 gram under section 202 for protecting sensitive personally  
 21 identifiable information.

22 (c) LIMITATIONS.—Notwithstanding any other obli-  
 23 gation under this subtitle, this subtitle does not apply to:

24 (1) FINANCIAL INSTITUTIONS.—Financial insti-  
 25 tutions—

(A) subject to the data security requirements and implementing regulations under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); and

(B) subject to—

(i) examinations for compliance with the requirements of this Act by a Federal Functional Regulator or State Insurance Authority (as those terms are defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)); or

(ii) compliance with part 314 of title 16, Code of Federal Regulations.

(2) HIPAA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

(B) BUSINESS ENTITIES.—A business entity shall be deemed in compliance with this Act if the business entity—

(i) is acting as a business associate, as that term is defined under the Health Insurance Portability and Accountability

1 Act of 1996 (42 U.S.C. 1301 et seq.) and  
2 is in compliance with the requirements im-  
3 posed under that Act and implementing  
4 regulations promulgated under that Act;  
5 and

6 (ii) is subject to, and currently in  
7 compliance, with the privacy and data se-  
8 curity requirements under sections 13401  
9 and 13404 of division A of the American  
10 Reinvestment and Recovery Act of 2009  
11 (42 U.S.C. 17931 and 17934) and imple-  
12 menting regulations promulgated under  
13 such sections.

14 (3) PUBLIC RECORDS.—Public records not oth-  
15 erwise subject to a confidentiality or nondisclosure  
16 requirement, or information obtained from a news  
17 report or periodical.

18 (d) RULE OF CONSTRUCTION.—Nothing in this sub-  
19 title shall be construed to modify, limit, or supersede the  
20 operation of the provisions of the Gramm-Leach-Bliley Act  
21 (15 U.S.C. 6801 et seq.), or its implementing regulations,  
22 including such regulations adopted or enforced by the  
23 States.

1 **SEC. 202. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**  
2 **AND SECURITY PROGRAM.**

3 (a) PERSONAL DATA PRIVACY AND SECURITY PRO-  
4 GRAM.—A business entity subject to this subtitle shall  
5 comply with the following safeguards and any other ad-  
6 ministrative, technical, or physical safeguards identified by  
7 the Federal Trade Commission in a rulemaking process  
8 pursuant to section 553 of title 5, United States Code,  
9 for the protection of sensitive personally identifiable infor-  
10 mation:

11 (1) SCOPE.—A business entity shall implement  
12 a comprehensive personal data privacy and security  
13 program that includes administrative, technical, and  
14 physical safeguards appropriate to the size and com-  
15 plexity of the business entity and the nature and  
16 scope of its activities.

17 (2) DESIGN.—The personal data privacy and  
18 security program shall be designed to—

19 (A) ensure the privacy, security, and con-  
20 fidentiality of sensitive personally identifiable  
21 information;

22 (B) protect against any anticipated  
23 vulnerabilities to the privacy, security, or integ-  
24 rity of sensitive personally identifiable informa-  
25 tion; and

1 (C) protect against unauthorized access or  
2 use of sensitive personally identifiable informa-  
3 tion that could create a significant risk of harm  
4 or fraud to any individual.

5 (3) RISK ASSESSMENT.—A business entity  
6 shall—

7 (A) identify reasonably foreseeable internal  
8 and external vulnerabilities that could result in  
9 unauthorized access, disclosure, use, or alter-  
10 ation of sensitive personally identifiable infor-  
11 mation or systems containing sensitive person-  
12 ally identifiable information;

13 (B) assess the likelihood of and potential  
14 damage from unauthorized access, disclosure,  
15 use, or alteration of sensitive personally identifi-  
16 able information;

17 (C) assess the sufficiency of its policies,  
18 technologies, and safeguards in place to control  
19 and minimize risks from unauthorized access,  
20 disclosure, use, or alteration of sensitive person-  
21 ally identifiable information; and

22 (D) assess the vulnerability of sensitive  
23 personally identifiable information during de-  
24 struction and disposal of such information, in-



1 including through the disposal or retirement of  
2 hardware.

3 (4) RISK MANAGEMENT AND CONTROL.—Each  
4 business entity shall—

5 (A) design its personal data privacy and  
6 security program to control the risks identified  
7 under paragraph (3); and

8 (B) adopt measures commensurate with  
9 the sensitivity of the data as well as the size,  
10 complexity, and scope of the activities of the  
11 business entity that—

12 (i) control access to systems and fa-  
13 cilities containing sensitive personally iden-  
14 tifiable information, including controls to  
15 authenticate and permit access only to au-  
16 thorized individuals;

17 (ii) detect, record, and preserve infor-  
18 mation relevant to actual and attempted  
19 fraudulent, unlawful, or unauthorized ac-  
20 cess, disclosure, use, or alteration of sen-  
21 sitive personally identifiable information,  
22 including by employees and other individ-  
23 uals otherwise authorized to have access;

24 (iii) protect sensitive personally identi-  
25 fiable information during use, trans-

mission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means (including as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section 682 of title 16, Code of Federal Regulations);

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers, diskettes, and other electronic media that contain sensitive personally identifiable information;

(v) trace access to records containing sensitive personally identifiable information so that the business entity can determine who accessed or acquired such sensitive personally identifiable information pertaining to specific individuals;

1                   (vi) ensure that no third party or cus-  
 2                   tomer of the business entity is authorized  
 3                   to access or acquire sensitive personally  
 4                   identifiable information without the busi-  
 5                   ness entity first performing sufficient due  
 6                   diligence to ascertain, with reasonable cer-  
 7                   tainty, that such information is being  
 8                   sought for a valid legal purpose; and

9                   (vii) minimize the amount of personal  
 10                  information maintained by the business en-  
 11                  tity, providing for the retention of such  
 12                  personal information only as reasonably  
 13                  needed for the business purposes of the  
 14                  business entity or as necessary to comply  
 15                  with any other provision of law.

16           (b) TRAINING.—Each business entity subject to this  
 17 subtitle shall take steps to ensure employee training and  
 18 supervision for implementation of the data security pro-  
 19 gram of the business entity.

20           (c) VULNERABILITY TESTING.—

21           (1) IN GENERAL.—Each business entity subject  
 22 to this subtitle shall take steps to ensure regular  
 23 testing of key controls, systems, and procedures of  
 24 the personal data privacy and security program to

1 detect, prevent, and respond to attacks or intrusions,  
2 or other system failures.

3 (2) FREQUENCY.—The frequency and nature of  
4 the tests required under paragraph (1) shall be de-  
5 termined by the risk assessment of the business enti-  
6 ty under subsection (a)(3).

7 (d) RELATIONSHIP TO SERVICE PROVIDERS.—In the  
8 event a business entity subject to this subtitle engages  
9 service providers not subject to this subtitle, such business  
10 entity shall—

11 (1) exercise appropriate due diligence in select-  
12 ing those service providers for responsibilities related  
13 to sensitive personally identifiable information, and  
14 take reasonable steps to select and retain service  
15 providers that are capable of maintaining appro-  
16 priate safeguards for the security, privacy, and in-  
17 tegrity of the sensitive personally identifiable infor-  
18 mation at issue; and

19 (2) require those service providers by contract  
20 to implement and maintain appropriate measures de-  
21 signed to meet the objectives and requirements gov-  
22 erning entities subject to section 201, this section,  
23 and subtitle B.

24 (e) PERIODIC ASSESSMENT AND PERSONAL DATA  
25 PRIVACY AND SECURITY MODERNIZATION.—Each busi-

1   ness entity subject to this subtitle shall on a regular basis  
 2   monitor, evaluate, and adjust, as appropriate its data pri-  
 3   vacy and security program in light of any relevant changes  
 4   in—

5           (1) technology;

6           (2) the sensitivity of personally identifiable in-  
 7   formation;

8           (3) internal or external threats to personally  
 9   identifiable information; and

10          (4) the changing business arrangements of the  
 11   business entity, such as—

12           (A) mergers and acquisitions;

13           (B) alliances and joint ventures;

14           (C) outsourcing arrangements;

15           (D) bankruptcy; and

16           (E) changes to sensitive personally identifi-  
 17   able information systems.

18          (f) IMPLEMENTATION TIMELINE.—Not later than 1  
 19   year after the date of enactment of this Act, a business  
 20   entity subject to the provisions of this subtitle shall imple-  
 21   ment a data privacy and security program pursuant to this  
 22   subtitle.

23   **SEC. 203. FEDERAL ENFORCEMENT.**

24          (a) CIVIL PENALTIES.—

1           (1) IN GENERAL.—The Attorney General may  
 2       bring a civil action in the appropriate United States  
 3       district court against any business entity that en-  
 4       gages in conduct constituting a violation of this sub-  
 5       title and, upon proof of such conduct by a prepon-  
 6       derance of the evidence, such business entity shall be  
 7       subject to a civil penalty of not more than \$5,000  
 8       per violation per day while such a violation exists,  
 9       with a maximum of \$20,000,000 per violation, un-  
 10      less such conduct is found to be willful or inten-  
 11      tional.

12           (2) INTENTIONAL OR WILLFUL VIOLATION.—A  
 13      business entity that intentionally or willfully violates  
 14      the provisions of this subtitle shall be subject to ad-  
 15      ditional penalties in the amount of \$5,000 per viola-  
 16      tion per day while such a violation exists.

17           (3) CONSIDERATIONS.—In determining the  
 18      amount of a civil penalty under this subsection, the  
 19      court shall take into account—

20                   (A) the degree of culpability of the busi-  
 21                   ness entity;

22                   (B) any prior violations of this subtitle by  
 23                   the business entity;

24                   (C) the ability of the business entity to pay  
 25                   a civil penalty;

1 (D) the effect on the ability of the business  
2 entity to continue to do business;

3 (E) the number of individuals whose per-  
4 sonally identifiable information was com-  
5 promised by the breach;

6 (F) the relative cost of compliance with  
7 this subtitle; and

8 (G) such other matters as justice may re-  
9 quire.

10 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
11 ERAL.—

12 (1) IN GENERAL.—If it appears that a business  
13 entity has engaged, or is engaged, in any act or  
14 practice constituting a violation of this subtitle, the  
15 Attorney General may petition an appropriate dis-  
16 trict court of the United States for an order—

17 (A) enjoining such act or practice; or

18 (B) enforcing compliance with this subtitle.

19 (2) ISSUANCE OF ORDER.—A court may issue  
20 an order under paragraph (1), if the court finds that  
21 the conduct in question constitutes a violation of this  
22 subtitle.

23 (c) OTHER RIGHTS AND REMEDIES.—The rights and  
24 remedies available under this section are cumulative and

1 shall not affect any other rights and remedies available  
2 under law.

3 **SEC. 204. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

4 (a) CIVIL ACTIONS.—

5 (1) IN GENERAL.—In any case in which the at-  
6 torney general of a State or any State or local law  
7 enforcement agency authorized by the State attorney  
8 general or by State statute to prosecute violations of  
9 consumer protection law, has reason to believe that  
10 an interest of the residents of that State has been  
11 or is threatened or adversely affected by the acts or  
12 practices of a business entity that violate this sub-  
13 title, the State may bring a civil action on behalf of  
14 the residents of that State in a district court of the  
15 United States of appropriate jurisdiction, or any  
16 other court of competent jurisdiction, to—

17 (A) enjoin that act or practice;

18 (B) enforce compliance with this subtitle;

19 or

20 (C) obtain civil penalties of not more than  
21 \$5,000 per violation per day while such viola-  
22 tions persist, up to a maximum of \$20,000,000  
23 per violation.



1           (2) CONSIDERATIONS.—In determining the  
2           amount of a civil penalty under this subsection, the  
3           court shall take into account—

4                   (A) the degree of culpability of the busi-  
5                   ness entity;

6                   (B) any prior violations of this subtitle by  
7                   the business entity;

8                   (C) the ability of the business entity to pay  
9                   a civil penalty;

10                  (D) the effect on the ability of the business  
11                  entity to continue to do business;

12                  (E) the number of individuals whose per-  
13                  sonally identifiable information was com-  
14                  promised by the breach;

15                  (F) the relative cost of compliance with  
16                  this subtitle; and

17                  (G) such other matters as justice may re-  
18                  quire.

19           (3) NOTICE.—

20                   (A) IN GENERAL.—Before filing an action  
21                   under this subsection, the attorney general of  
22                   the State involved shall provide to the Attorney  
23                   General—

24                           (i) a written notice of that action; and

1 (ii) a copy of the complaint for that  
2 action.

3 (B) EXEMPTION.—

4 (i) IN GENERAL.—Subparagraph (A)  
5 shall not apply with respect to the filing of  
6 an action by an attorney general of a State  
7 under this subsection, if the attorney gen-  
8 eral of a State determines that it is not  
9 feasible to provide the notice described in  
10 this subparagraph before the filing of the  
11 action.

12 (ii) NOTIFICATION.—In an action de-  
13 scribed in clause (i), the attorney general  
14 of a State shall provide notice and a copy  
15 of the complaint to the Attorney General  
16 at the time the State attorney general files  
17 the action.

18 (b) FEDERAL PROCEEDINGS.—Upon receiving notice  
19 under subsection (a)(2), the Attorney General shall have  
20 the right to—

21 (1) move to stay the action, pending the final  
22 disposition of a pending Federal proceeding or ac-  
23 tion;

24 (2) initiate an action in the appropriate United  
25 States district court under section 217 and move to

1        consolidate all pending actions, including State ac-  
2        tions, in such court;

3            (3) intervene in an action brought under sub-  
4        section (a)(2); and

5            (4) file petitions for appeal.

6        (c) PENDING PROCEEDINGS.—If the Attorney Gen-  
7        eral has instituted a proceeding or action for a violation  
8        of this subtitle or any regulations thereunder, no attorney  
9        general of a State may, during the pendency of such pro-  
10       ceeding or action, bring an action under this subtitle  
11       against any defendant named in such criminal proceeding  
12       or civil action for any violation that is alleged in that pro-  
13       ceeding or action.

14       (d) CONSTRUCTION.—For purposes of bringing any  
15       civil action under subsection (a), nothing in this subtitle  
16       regarding notification shall be construed to prevent an at-  
17       torney general of a State from exercising the powers con-  
18       ferred on such attorney general by the laws of that State  
19       to—

20            (1) conduct investigations;

21            (2) administer oaths or affirmations; or

22            (3) compel the attendance of witnesses or the  
23       production of documentary and other evidence.

24       (e) VENUE; SERVICE OF PROCESS.—

1           (1) VENUE.—Any action brought under sub-  
2           section (a) may be brought in—

3                   (A) the district court of the United States  
4                   that meets applicable requirements relating to  
5                   venue under section 1391 of title 28, United  
6                   States Code; or

7                   (B) another court of competent jurisdic-  
8                   tion.

9           (2) SERVICE OF PROCESS.—In an action  
10          brought under subsection (a), process may be served  
11          in any district in which the defendant—

12                   (A) is an inhabitant; or

13                   (B) may be found.

14 **SEC. 205. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.**

15          (a) IN GENERAL.—Any person aggrieved by a viola-  
16          tion of the provisions of this subtitle by a business entity  
17          may bring a civil action in a court of appropriate jurisdic-  
18          tion to recover for personal injuries sustained as a result  
19          of the violation.

20          (b) AUTHORITY TO BRING CIVIL ACTION; JURISDIC-  
21          TION.—As provided in subsection (c), any person may  
22          commence a civil action on his own behalf against any  
23          business entity who is alleged to have violated the provi-  
24          sions of this subtitle.

25          (c) REMEDIES IN A CITIZEN SUIT.—

1           (1) DAMAGES.—Any individual harmed by a  
2           failure of a business entity to comply with the provi-  
3           sions of this subtitle, shall be able to collect damages  
4           of not more than \$10,000 per violation per day while  
5           such violations persist, up to a maximum of  
6           \$20,000,000 per violation.

7           (2) PUNITIVE DAMAGES.—A business entity  
8           may be liable for punitive damages if the business  
9           entity intentionally or willfully violates the provisions  
10          of this subtitle.

11          (3) EQUITABLE RELIEF.—A business entity  
12          that violates the provisions of this subtitle may be  
13          enjoined to comply with the provisions of those sec-  
14          tions.

15          (d) OTHER RIGHTS AND REMEDIES.—The rights and  
16          remedies available under this subsection are cumulative  
17          and shall not affect any other rights and remedies avail-  
18          able under law.

19          (e) ACCESS TO JUSTICE.—The rights and remedies  
20          afforded by this section shall not be abridged or precluded  
21          by any predispute arbitration agreement, and any claims  
22          under this section that arise from the same security  
23          breach are presumed to meet the commonality require-  
24          ment under rule 23(a)(2) of the Federal Rules of Civil  
25          Procedure.

## **Subtitle B—Security Breach Notification**

### **SEC. 211. NOTICE TO INDIVIDUALS.**

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information that experiences a security breach of such information, shall, following the discovery of such security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

#### **(b) OBLIGATION OF OWNER OR LICENSEE.—**

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall prevent or abrogate an agreement between an agency or business entity required to give notice

1 under this section and a designated third party, in-  
2 cluding an owner or licensee of the sensitive person-  
3 ally identifiable information subject to the security  
4 breach, to provide the notifications required under  
5 subsection (a).

6 (3) BUSINESS ENTITY RELIEVED FROM GIVING  
7 NOTICE.—A business entity obligated to give notice  
8 under subsection (a) shall be relieved of such obliga-  
9 tion if an owner or licensee of the sensitive person-  
10 ally identifiable information subject to the security  
11 breach, or other designated third party, provides  
12 such notification.

13 (c) TIMELINESS OF NOTIFICATION.—

14 (1) IN GENERAL.—All notifications required  
15 under this section shall be made without unreason-  
16 able delay following the discovery by the agency or  
17 business entity of a security breach.

18 (2) REASONABLE DELAY.—Reasonable delay  
19 under this subsection may include any time nec-  
20 essary to determine the scope of the security breach,  
21 conduct the risk assessment described in section  
22 212(b)(1), and provide notice to law enforcement  
23 when required.

24 (3) BURDEN OF PRODUCTION.—The agency,  
25 business entity, owner, or licensee required to pro-

1       vide notice under this subtitle shall, upon the re-  
2       quest of the Attorney General or the attorney gen-  
3       eral of a State or any State or local law enforcement  
4       agency authorized by the attorney general of the  
5       State or by State statute to prosecute violations of  
6       consumer protection law, provide records or other  
7       evidence of the notifications required under this sub-  
8       title, including to the extent applicable, the reasons  
9       for any delay of notification.

10       (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW  
11       ENFORCEMENT PURPOSES.—

12               (1) IN GENERAL.—If a Federal law enforce-  
13       ment agency or member of the intelligence commu-  
14       nity determines that the notification required under  
15       this section would impede any lawfully authorized  
16       criminal investigation or authorized investigative,  
17       protective, or intelligence activities that are carried  
18       out by or on behalf of any element of the intelligence  
19       community and conducted in accordance with the  
20       United States laws, authorities, and regulations gov-  
21       erning such intelligence activities, such notification  
22       shall be delayed upon written notice from such Fed-  
23       eral law enforcement or intelligence agency to the  
24       agency or business entity that experienced the  
25       breach.



1           (2) EXTENDED DELAY OF NOTIFICATION.—If  
2           the notification required under subsection (a) is de-  
3           layed pursuant to paragraph (1), an agency or busi-  
4           ness entity shall give notice 30 days after the day  
5           such law enforcement delay was invoked unless a  
6           Federal law enforcement or intelligence agency pro-  
7           vides written notification that further delay is nec-  
8           essary.

9           (3) LAW ENFORCEMENT IMMUNITY.—No cause  
10          of action shall lie in any court against any law en-  
11          forcement agency for acts relating to the delay of  
12          notification for law enforcement or intelligence pur-  
13          poses under this subtitle.

14 **SEC. 212. EXEMPTIONS FROM NOTICE TO INDIVIDUALS.**

15          (a) EXEMPTION FOR NATIONAL SECURITY AND LAW  
16          ENFORCEMENT.—

17               (1) IN GENERAL.—Section 211 shall not apply  
18               to an agency or business entity if the agency or busi-  
19               ness entity certifies, in writing, that notification of  
20               the security breach as required by section 211 rea-  
21               sonably could be expected to—

22                       (A) cause damage to the national security;  
23                       or

1 (B) hinder a law enforcement investigation  
2 or the ability of the agency to conduct law en-  
3 forcement investigations.

4 (2) LIMITS ON CERTIFICATIONS.—An agency or  
5 business entity may not execute a certification under  
6 paragraph (1) to—

7 (A) conceal violations of law, inefficiency,  
8 or administrative error;

9 (B) prevent embarrassment to a business  
10 entity, organization, or agency;

11 (C) restrain competition; or

12 (D) delay notification under section 211  
13 for any other reason, except where the agency  
14 or business entity reasonably believes an exemp-  
15 tion under paragraph (1) applies.

16 (3) NOTICE.—In every case in which an agency  
17 or business agency issues a certification under para-  
18 graph (1), the certification, accompanied by a de-  
19 scription of the factual basis for the certification,  
20 shall be immediately provided to the United States  
21 Secret Service and the Federal Bureau of Investiga-  
22 tion.

23 (4) SECRET SERVICE AND FBI REVIEW OF CER-  
24 TIFICATIONS.—

1           (A) IN GENERAL.—The United States Se-  
2           cret Service or the Federal Bureau of Investiga-  
3           tion may review a certification provided by an  
4           agency under paragraph (3), and shall review a  
5           certification provided by a business entity under  
6           paragraph (3), to determine whether an exemp-  
7           tion under paragraph (1) is merited. Such re-  
8           view shall be completed not later than 7 busi-  
9           ness days after the date of receipt of the certifi-  
10          cation, except as provided in paragraph (5)(C).

11          (B) NOTICE.—Upon completing a review  
12          under subparagraph (A) the United States Se-  
13          cret Service or the Federal Bureau of Investiga-  
14          tion shall immediately notify the agency or  
15          business entity, in writing, of its determination  
16          of whether an exemption under paragraph (1)  
17          is merited.

18          (C) EXEMPTION.—The exemption under  
19          paragraph (1) shall not apply if the United  
20          States Secret Service or the Federal Bureau of  
21          Investigation determines under this paragraph  
22          that the exemption is not merited.

23          (5) ADDITIONAL AUTHORITY OF THE SECRET  
24          SERVICE AND FBI.—

1 (A) IN GENERAL.—In determining under  
2 paragraph (4) whether an exemption under  
3 paragraph (1) is merited, the United States Se-  
4 cret Service or the Federal Bureau of Investiga-  
5 tion may request additional information from  
6 the agency or business entity regarding the  
7 basis for the claimed exemption, if such addi-  
8 tional information is necessary to determine  
9 whether the exemption is merited.

10 (B) REQUIRED COMPLIANCE.—Any agency  
11 or business entity that receives a request for  
12 additional information under subparagraph (A)  
13 shall cooperate with any such request.

14 (C) TIMING.—If the United States Secret  
15 Service or the Federal Bureau of Investigation  
16 requests additional information under subpara-  
17 graph (A), the United States Secret Service or  
18 the Federal Bureau of Investigation shall notify  
19 the agency or business entity not later than 7  
20 business days after the date of receipt of the  
21 additional information whether an exemption  
22 under paragraph (1) is merited.

23 (b) SAFE HARBOR.—

1           (1) IN GENERAL.—An agency or business entity  
2     will be exempt from the notice requirements under  
3     section 211, if—

4           (A) a risk assessment conducted by the  
5     agency or business entity concludes that there  
6     is no significant risk that a security breach has  
7     resulted in, or will result in harm to the individ-  
8     uals whose sensitive personally identifiable in-  
9     formation was subject to the security breach;  
10    and

11          (B) the United States Secret Service or the  
12     Federal Bureau of Investigation does not indi-  
13     cate within 7 business days from the receipt of  
14     written notification from an agency or business  
15     entity pursuant to subsection (b)(2), that the  
16     agency or business entity should not be exempt  
17     from the notice requirements of section 211.

18          (2) RISK ASSESSMENT REQUIREMENTS.—

19          (A) CONDUCTING A RISK ASSESSMENT.—  
20     Upon discovery of a security breach of an agen-  
21     cy or business entity, the agency or business en-  
22     tity shall conduct a risk assessment to deter-  
23     mine if there is a significant risk that the secu-  
24     rity breach resulted in, or will result in, harm  
25     to the individuals whose sensitive personally

1 identifiable information was subject to the secu-  
2 rity breach.

3 (i) PRESUMPTION OF NO SIGNIFICANT  
4 RISK.—It is presumed that there is no sig-  
5 nificant risk that the security breach has  
6 resulted in, or will result in, harm to the  
7 individuals whose sensitive personally iden-  
8 tifiable information was subject to the se-  
9 curity breach, if such sensitive personally  
10 identifiable information has been rendered  
11 indecipherable through the use of best  
12 practices or methods as described by the  
13 Federal Trade Commission, such as redac-  
14 tion, access controls, or other such mecha-  
15 nisms, which are widely accepted as an ef-  
16 fective industry practice, or an effective in-  
17 dustry standard, or other such mechanisms  
18 establishing a presumption that no signifi-  
19 cant risk exists.

20 (ii) PRESUMPTION OF SIGNIFICANT  
21 RISK.—It is presumed that there is a sig-  
22 nificant risk that the security breach has  
23 resulted in, or will result in, harm to indi-  
24 viduals whose sensitive personally identifi-  
25 able information was subject to the secu-

1           rity breach if the agency or business entity  
2           failed to render such sensitive personally  
3           identifiable information indecipherable  
4           through the use of best practices or meth-  
5           ods, such as redaction, access controls, or  
6           other such mechanisms which are widely  
7           accepted as an effective industry practice  
8           or an effective industry standard, or other  
9           such mechanisms establishing a presump-  
10          tion that a significant risk exists.

11           (B) WRITTEN NOTIFICATION TO LAW EN-  
12          FORCEMENT.—Without unreasonable delay, but  
13          not later than 7 days after the discovery of a  
14          security breach, unless extended by the United  
15          States Secret Service or the Federal Bureau of  
16          Investigation, the agency or business entity  
17          must notify the United States Secret Service  
18          and the Federal Bureau of Investigation, in  
19          writing, of—

20                   (i) the results of the risk assessment;

21                   and

22                   (ii) its decision to invoke the risk as-  
23                   sessment exemption.

24          (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

1           (1) IN GENERAL.—A business entity shall be  
2       exempt from the notice requirement under section  
3       211 if the business entity utilizes or participates in  
4       a security program that—

5           (A) is designed to block the use of the sen-  
6       sitive personally identifiable information to ini-  
7       tiate unauthorized financial transactions before  
8       they are charged to the account of the indi-  
9       vidual; and

10          (B) provides for notice to affected individ-  
11       uals after a security breach that has resulted in  
12       fraud or unauthorized transactions.

13          (2) LIMITATION.—Paragraph (1) does not  
14       apply to a business entity if—

15          (A) the information subject to the security  
16       breach includes sensitive personally identifiable  
17       information, other than a credit card or credit  
18       card security code, of any type of the sensitive  
19       personally identifiable information identified in  
20       section 3; or

21          (B) the security breach includes both the  
22       individual's credit card number and the individ-  
23       ual's first and last name.



1 **SEC. 213. METHODS OF NOTICE TO INDIVIDUALS.**

2 To comply with section 211, an agency or business  
3 entity shall provide the following forms of notice:

4 (1) INDIVIDUAL WRITTEN NOTICE.—Written  
5 notice to individuals by 1 of the following means:

6 (A) Individual written notification to the  
7 last known home mailing address of the indi-  
8 vidual in the records of the agency or business  
9 entity.

10 (B) E-mail notice, unless the individual  
11 has expressly opted not to receive such notices  
12 of security breaches or the notice is inconsistent  
13 with the provisions permitting electronic trans-  
14 mission of notices under section 101 of the  
15 Electronic Signatures in Global and National  
16 Commerce Act (15 U.S.C. 7001).

17 (2) TELEPHONE NOTICE.—Telephone notice to  
18 the individual personally.

19 (3) PUBLIC NOTICE.—

20 (A) ELECTRONIC NOTICE.—Prominent no-  
21 tice via all reasonable means of electronic con-  
22 tact between the individual and the agency or  
23 business entity, including any website,  
24 networked devices, or other interface through  
25 which the agency or business entity regularly  
26 interacts with the consumer, if the number of

1 individuals whose personally identifiable infor-  
2 mation was or is reasonably believed to have  
3 been accessed or acquired by an unauthorized  
4 person exceeds 5,000.

5 (B) MEDIA NOTICE.—Notice to major  
6 media outlets serving a State or jurisdiction, if  
7 the number of residents of such State whose  
8 sensitive personally identifiable information  
9 was, or is reasonably believed to have been,  
10 accessed or acquired by an unauthorized person  
11 exceeds 5,000.

12 **SEC. 214. CONTENT OF NOTICE TO INDIVIDUALS.**

13 (a) IN GENERAL.—Regardless of the method by  
14 which individual notice is provided to individuals under  
15 section 213(1), such notice shall include—

16 (1) a description of the categories of sensitive  
17 personally identifiable information that was, or is  
18 reasonably believed to have been, accessed or ac-  
19 quired by an unauthorized person, and how the  
20 agency or business entity came into possession the  
21 sensitive personally identifiable information at issue;

22 (2) a toll-free number—

23 (A) that the individual may use to contact  
24 the agency or business entity, or the agent of  
25 the agency or business entity; and

1 (B) from which the individual may learn  
2 what types of sensitive personally identifiable  
3 information the agency or business entity main-  
4 tained about that individual;

5 (3) the toll-free contact telephone numbers,  
6 websites, and addresses for the major credit report-  
7 ing agencies;

8 (4) the telephone numbers and websites for the  
9 relevant Federal agencies that provide information  
10 regarding identity theft prevention and protection;

11 (5) notice that the individual is entitled to re-  
12 ceive, at no cost to such individual, consumer credit  
13 reports on a quarterly basis for a period of 2 years,  
14 credit monitoring or any other service that enables  
15 consumers to detect the misuse of sensitive person-  
16 ally identifiable information for a period of 2 years,  
17 and instructions to the individual on requesting such  
18 reports or service from the agency or business enti-  
19 ty;

20 (6) notice that the individual is entitled to re-  
21 ceive a security freeze and that the agency or busi-  
22 ness entity will be liable for any costs associated  
23 with the security freeze for 2 years and the nec-  
24 essary instructions for requesting a security freeze;  
25 and

1           (7) notice that any costs or damages incurred  
2       by an individual as a result of a security breach will  
3       be paid by the business entity or agency that experi-  
4       enced the security breach.

5       (b) TELEPHONE NOTICE.—Telephone notice de-  
6       scribed in section 213(2) shall include, to the extent pos-  
7       sible—

8           (1) notification that a security breach has oc-  
9       curred and that the individual’s sensitive personally  
10      identifiable information may have been com-  
11      promised;

12          (2) a description of the categories of sensitive  
13      personally identifiable information that were, or are  
14      reasonably believed to have been, accessed or ac-  
15      quired by an unauthorized person;

16          (3) a toll-free number and website—

17              (A) that the individual may use to contact  
18      the agency or business entity, or the authorized  
19      agent of the agency or business entity; and

20              (B) from which the individual may learn  
21      what types of sensitive personally identifiable  
22      information the agency or business entity main-  
23      tained about that individual and remedies avail-  
24      able to that individual; and

1           (4) an alert to the individual that the agency or  
2       business entity is sending or has sent written notifi-  
3       cation containing additional information as required  
4       under section 213(1)(A).

5       (c) PUBLIC NOTICE.—Public notice described in sec-  
6       tion 213(3) shall include—

7           (1) electronic notice, which includes—

8               (A) notification that a security breach has  
9               occurred and that the individual’s sensitive per-  
10              sonally identifiable information may have been  
11              compromised;

12              (B) a description of the categories of sen-  
13              sitive personally identifiable information that  
14              were, or are reasonably believed to have been,  
15              accessed or acquired by an unauthorized per-  
16              son; and

17              (C) a toll-free number and website—

18                      (i) that the individual may use to con-  
19                      tact the agency or business entity, or the  
20                      authorized agent of the agency or business  
21                      entity; and

22                      (ii) from which the individual may  
23                      learn what types of sensitive personally  
24                      identifiable information the agency or busi-  
25                      ness entity maintained about that indi-

1           vidual and remedies available to that indi-  
2           vidual;

3           (2) media notice, which includes—

4               (A) a description of the categories of sen-  
5               sitive personally identifiable information that  
6               was, or is reasonably believed to have been,  
7               accessed or acquired by an unauthorized per-  
8               son;

9               (B) a toll-free number—

10                   (i) that the individual may use to con-  
11                   tact the agency or business entity, or the  
12                   authorized agent of the agency or business  
13                   entity; and

14                   (ii) from which the individual may  
15                   learn what types of sensitive personally  
16                   identifiable information the agency or busi-  
17                   ness entity maintained about that indi-  
18                   vidual and remedies available to that indi-  
19                   vidual;

20               (C) the toll-free contact telephone num-  
21               bers, websites, and addresses for the major  
22               credit reporting agencies;

23               (D) the telephone numbers and websites  
24               for the relevant Federal agencies that provide

1 information regarding identity theft prevention  
2 and protection;

3 (E) notice that the affected individuals are  
4 entitled to receive, at no cost to such individ-  
5 uals, consumer credit reports on a quarterly  
6 basis for a period of 2 years, credit monitoring,  
7 or any other service that enables consumers to  
8 detect the misuse of sensitive personally identi-  
9 fiable information for a period of 2 years;

10 (F) notice that the individual is entitled to  
11 receive a security freeze and that the agency or  
12 business entity will be liable for any costs asso-  
13 ciated with the security freeze for 2 years; and

14 (G) notice that the individual is entitled to  
15 receive compensation from the business entity  
16 or agency for any costs or damages incurred by  
17 the individual resulting from the security  
18 breach.

19 (d) **ADDITIONAL CONTENT.**—Notwithstanding sec-  
20 tion 221, a State may require that a notice under sub-  
21 section (a) shall also include information regarding victim  
22 protection assistance provided for by that State.

23 **SEC. 215. REMEDIES FOR SECURITY BREACH.**

24 (a) **CREDIT REPORTS AND CREDIT MONITORING.**—  
25 An agency or business entity required to provide notifica-

1 tion under this subtitle shall, upon request of an individual  
2 whose sensitive personally identifiable information was in-  
3 cluded in the security breach, provide or arrange for the  
4 provision of, to each such individual and at no cost to such  
5 individual—

6 (1) consumer credit reports from not fewer  
7 than 1 of the major credit reporting agencies begin-  
8 ning not later than 60 days following the request of  
9 the individual and continuing on a quarterly basis  
10 for a period of 2 years thereafter; and

11 (2) a credit monitoring or other service that en-  
12 ables consumers to detect the misuse of their per-  
13 sonal information, beginning not later than 60 days  
14 following the request of the individual and con-  
15 tinuing for a period of 2 years.

16 (b) SECURITY FREEZE.—

17 (1) REQUEST.—Any consumer may submit a  
18 written request, by certified mail or such other se-  
19 cure method as authorized by a credit rating agency,  
20 to a credit rating agency to place a security freeze  
21 on the credit report of the consumer.

22 (2) IMPLEMENTATION OF SECURITY FREEZE.—  
23 Upon receipt of a written request under paragraph  
24 (1), a credit rating agency shall—



1 (A) not later than 5 business days after re-  
2 ceipt of the request, place a security freeze on  
3 the credit report of the consumer; and

4 (B) not later than 10 business days after  
5 placing a security freeze, send a written con-  
6 firmation of such security freeze to the con-  
7 sumer, which shall provide the consumer with a  
8 unique personal identification number or pass-  
9 word to be used by the consumer when pro-  
10 viding authorization for the release of the credit  
11 report of the consumer to a third party or for  
12 a specified period of time.

13 (3) DURATION OF SECURITY FREEZE.—Except  
14 as provided in paragraph (4), any security freeze au-  
15 thorized pursuant to the provisions of this section  
16 shall remain in effect until the consumer requests  
17 security freeze to be removed.

18 (4) DISCLOSURE OF CREDIT REPORT TO THIRD  
19 PARTY.—

20 (A) IN GENERAL.—If a consumer that has  
21 requested a security freeze under this sub-  
22 section wishes to authorize the disclosure of the  
23 credit report of the consumer to a third party,  
24 or for a specified period of time, while such se-

1 security freeze is in effect, the consumer shall  
2 contact the credit rating agency and provide—

3 (i) proper identification;

4 (ii) the unique personal identification  
5 number or password described in para-  
6 graph (2)(B); and

7 (iii) proper information regarding the  
8 third party who is to receive the credit re-  
9 port or the time period for which the credit  
10 report shall be available.

11 (B) REQUIREMENT.—Not later than 3  
12 business days after receipt of a request under  
13 subparagraph (A), a credit rating agency shall  
14 lift the security freeze.

15 (5) PROCEDURES.—

16 (A) IN GENERAL.—A credit rating agency  
17 shall develop procedures to receive and process  
18 requests from consumers under paragraph (2)  
19 of this section.

20 (B) REQUIREMENT.—Procedures developed  
21 under subparagraph (A), at a minimum, shall  
22 include the ability of a consumer to send such  
23 temporary lift or removal request by electronic  
24 mail, letter, telephone, or facsimile.

1           (6) REQUESTS BY THIRD PARTY.—If a third  
2           party requests access to a credit report of a con-  
3           sumer that has been frozen under this subsection  
4           and the consumer has not authorized the disclosure  
5           of the credit report of the consumer to the third  
6           party, the third party may deem such credit applica-  
7           tion as incomplete.

8           (7) DETERMINATION BY CREDIT RATING AGEN-  
9           CY.—

10           (A) IN GENERAL.—A credit rating agency  
11           may refuse to implement or may remove a secu-  
12           rity freeze under this subsection if the agency  
13           determines, in good faith, that—

14                   (i) the request for a security freeze  
15                   was made as part of a fraud that the con-  
16                   sumer participated in, had knowledge of,  
17                   or that can be demonstrated by cir-  
18                   cumstantial evidence; or

19                   (ii) the consumer credit report was  
20                   frozen due to a material misrepresentation  
21                   of fact by the consumer.

22           (B) NOTICE.—If a credit rating agency  
23           makes a determination under subparagraph (A)  
24           to not implement, or to remove, a security  
25           freeze under this subsection, the credit rating

1           agency shall notify the consumer in writing of  
2           such determination—

3                   (i) in the case of a determination not  
4                   to implement a security freeze, not later  
5                   than 5 business days after the determina-  
6                   tion is made; and

7                   (ii) in the case of a removal of a secu-  
8                   rity freeze, prior to removing the freeze on  
9                   the credit report of the consumer.

10           (8) RULE OF CONSTRUCTION.—Nothing in this  
11           section shall be construed to prohibit disclosure of a  
12           credit report of a consumer to—

13                   (A) a person, or the person's subsidiary,  
14                   affiliate, agent or assignee with which the con-  
15                   sumer has or, prior to assignment, had an ac-  
16                   count, contract or debtor-creditor relationship  
17                   for the purpose of reviewing the account or col-  
18                   lecting the financial obligation owing for the ac-  
19                   count, contract or debt;

20                   (B) a subsidiary, affiliate, agent, assignee  
21                   or prospective assignee of a person to whom ac-  
22                   cess has been granted under paragraph (4) for  
23                   the purpose of facilitating the extension of cred-  
24                   it or other permissible use;

1 (C) any person acting pursuant to a court  
2 order, warrant or subpoena;

3 (D) any person for the purpose of using  
4 such credit information to prescreen as provided  
5 by the Fair Credit Reporting Act (15 U.S.C.  
6 1681 et seq.);

7 (E) any person for the sole purpose of pro-  
8 viding a credit file monitoring subscription serv-  
9 ice to which the consumer has subscribed;

10 (F) a credit rating agency for the sole pur-  
11 pose of providing a consumer with a copy of the  
12 credit report of the consumer upon the request  
13 of the consumer; or

14 (G) a Federal, State or local governmental  
15 entity, including a law enforcement agency, or  
16 court, or their agents or assignees pursuant to  
17 their statutory or regulatory duties. For pur-  
18 poses of this subsection, “reviewing the ac-  
19 count” includes activities related to account  
20 maintenance, monitoring, credit line increases  
21 and account upgrades and enhancements; and

22 (H) any person for the sole purpose of pro-  
23 viding a remedy requested by an individual  
24 under this section.

1           (9) EXCEPTIONS.—The following persons shall  
2       not be required to place a security freeze under this  
3       subsection, but shall be subject to any security  
4       freeze placed on a credit report by another credit  
5       rating agency:

6           (A) A check services or fraud prevention  
7       services company that reports on incidents of  
8       fraud or issues authorizations for the purpose  
9       of approving or processing negotiable instru-  
10      ments, electronic fund transfers or similar  
11      methods of payment.

12          (B) A deposit account information service  
13      company that issues reports regarding account  
14      closures due to fraud, substantial overdrafts,  
15      automated teller machine abuse, or similar in-  
16      formation regarding a consumer to inquiring  
17      banks or other financial institutions for use  
18      only in reviewing a consumer request for a de-  
19      posit account at the inquiring bank or financial  
20      institution.

21          (C) A credit rating agency that—

22              (i) acts only to resell credit informa-  
23              tion by assembling and merging informa-  
24              tion contained in a database of 1 or more  
25              credit reporting agencies; and

1 (ii) does not maintain a permanent  
2 database of credit information from which  
3 new credit reports are produced.

4 (10) FEES.—

5 (A) IN GENERAL.—A credit rating agency  
6 may charge reasonable fees for each security  
7 freeze, removal of such freeze or temporary lift  
8 of such freeze for a period of time, and a tem-  
9 porary lift of such freeze for a specific party.

10 (B) REQUIREMENT.—Any fees charged  
11 under subparagraph (A) shall be borne by the  
12 agency or business entity providing notice under  
13 section 214 for 2 years following the establish-  
14 ment of the security freeze under this sub-  
15 section.

16 (c) COSTS RESULTING FROM A SECURITY  
17 BREACH.—

18 (1) IN GENERAL.—A business entity or agency  
19 that experiences a security breach and is required to  
20 provide notice under this subtitle shall pay, upon re-  
21 quest, to any individual whose sensitive personally  
22 identifiable information has been, or is reasonably  
23 believed to have been, accessed or acquired as a re-  
24 sult of such security breach, any costs or damages  
25 incurred by the individual as a result of such secu-

1        rity breach, including costs associated with identity  
2        theft suffered as a result of such security breach.

3            (2) COMPLIANCE.—A business entity or agency  
4        shall be deemed in compliance with this subsection  
5        if the business entity or agency—

6            (A) provides insurance to any individual  
7        whose sensitive personally identifiable informa-  
8        tion has been, or is reasonably believed to have  
9        been, accessed or acquired as a result of a secu-  
10       rity breach and such insurance is sufficient to  
11       compensate the consumer for not less than  
12       \$25,000 of costs or damages; or

13           (B) pays, without unreasonable delay, any  
14        actual costs or damages incurred by an indi-  
15       vidual as a result of the security breach.

16   **SEC. 216. NOTICE TO CREDIT REPORTING AGENCIES.**

17        If an agency or business entity is required to provide  
18       notification to more than 5,000 individuals under section  
19       211(a), the agency or business entity shall also notify all  
20       consumer reporting agencies that compile and maintain  
21       files on consumers on a nationwide basis (as defined in  
22       section 603(p) of the Fair Credit Reporting Act (15  
23       U.S.C. 1681a(p)) of the timing and distribution of the no-  
24       tices. Such notice shall be given to the consumer credit  
25       reporting agencies without unreasonable delay and, if it



1 will not delay notice to the affected individuals, prior to  
2 the distribution of notices to the affected individuals.

3 **SEC. 217. NOTICE TO LAW ENFORCEMENT.**

4 (a) SECRET SERVICE AND FBI.—Any business entity  
5 or agency shall notify the United States Secret Service  
6 and the Federal Bureau of Investigation of the fact that  
7 a security breach has occurred if—

8 (1) the number of individuals whose sensitive  
9 personally identifying information was, or is reason-  
10 ably believed to have been accessed or acquired by  
11 an unauthorized person exceeds 5,000;

12 (2) the security breach involves a database,  
13 networked or integrated databases, or other data  
14 system containing the sensitive personally identifi-  
15 able information of more than 500,000 individuals  
16 nationwide;

17 (3) the security breach involves databases  
18 owned by the Federal Government; or

19 (4) the security breach involves primarily sen-  
20 sitive personally identifiable information of individ-  
21 uals known to the agency or business entity to be  
22 employees and contractors of the Federal Govern-  
23 ment involved in national security or law enforce-  
24 ment.

1 (b) FTC REVIEW OF THRESHOLDS.—The Federal  
2 Trade Commission may alter the circumstances under  
3 which notification is required under subsection (a) in a  
4 matter consistent with the public interest.

5 (c) NOTICE TO OTHER LAW ENFORCEMENT AGEN-  
6 CIES.—The United States Secret Service and the Federal  
7 Bureau of Investigation shall be responsible for noti-  
8 fying—

9 (1) the United States Postal Inspection Service,  
10 if the security breach involves mail fraud;

11 (2) the attorney general of each State affected  
12 by the security breach; and

13 (3) the Federal Trade Commission, if the secu-  
14 rity breach involves consumer reporting agencies  
15 subject to the Fair Credit Reporting Act (15 U.S.C.  
16 1681 et seq.), or anticompetitive conduct.

17 (d) TIMING OF NOTICES.—The notices required  
18 under this section shall be delivered as follows:

19 (1) Notice under subsection (a) shall be deliv-  
20 ered as promptly as possible, but not later than 10  
21 days after discovery of the security breach.

22 (2) Notice under section 211 shall be delivered  
23 to individuals not later than 48 hours after the Fed-  
24 eral Bureau of Investigation or the Secret Service

1 receives notice of a security breach from an agency  
2 or business entity.

3 **SEC. 218. FEDERAL ENFORCEMENT.**

4 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—

5 (1) IN GENERAL.—The Attorney General may  
6 bring a civil action in the appropriate United States  
7 district court against any business entity that en-  
8 gages in conduct constituting a violation of this sub-  
9 title and, upon proof of such conduct by a prepon-  
10 derance of the evidence, such business entity shall be  
11 subject to a civil penalty of not more than \$500 per  
12 day per individual whose sensitive personally identi-  
13 fiable information was, or is reasonably believed to  
14 have been, accessed or acquired by an unauthorized  
15 person, up to a maximum of \$20,000,000 per viola-  
16 tion, unless such conduct is found to be willful or in-  
17 tentional.

18 (2) PRESUMPTION.—A violation of section  
19 212(a)(2) shall be presumed to be willful or inten-  
20 tional conduct.

21 (b) CONSIDERATIONS.—In determining the amount  
22 of a civil penalty under this subsection, the court shall  
23 take into account—

24 (1) the degree of culpability of the business en-  
25 tity;

1           (2) any prior violations of this subtitle by the  
2       business entity;

3           (3) the ability of the business entity to pay a  
4       civil penalty;

5           (4) the effect on the ability of the business enti-  
6       ty to continue to do business;

7           (5) the number of individuals whose personally  
8       identifiable information was compromised by the  
9       breach;

10          (6) the relative cost of compliance with this  
11       subtitle; and

12          (7) such other matters as justice may require.

13       (c) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-  
14       ERAL.—

15           (1) IN GENERAL.—If it appears that a business  
16       entity has engaged, or is engaged, in any act or  
17       practice constituting a violation of this subtitle, the  
18       Attorney General may petition an appropriate dis-  
19       trict court of the United States for an order—

20                   (A) enjoining such act or practice; or

21                   (B) enforcing compliance with this subtitle.

22           (2) ISSUANCE OF ORDER.—A court may issue  
23       an order under paragraph (1), if the court finds that  
24       the conduct in question constitutes a violation of this  
25       subtitle.

1 (d) OTHER RIGHTS AND REMEDIES.—The rights and  
 2 remedies available under this subtitle are cumulative and  
 3 shall not affect any other rights and remedies available  
 4 under law.

5 (e) FRAUD ALERT.—Section 605A(b)(1) of the Fair  
 6 Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is  
 7 amended by inserting “, or evidence that the consumer  
 8 has received notice that the consumer’s financial informa-  
 9 tion has or may have been compromised,” after “identity  
 10 theft report”.

11 **SEC. 219. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

12 (a) IN GENERAL.—

13 (1) CIVIL ACTIONS.—

14 (A) IN GENERAL.—In any case in which  
 15 the attorney general of a State or any State or  
 16 local law enforcement agency authorized by the  
 17 State attorney general or by State statute to  
 18 prosecute violations of consumer protection law,  
 19 has reason to believe that an interest of the  
 20 residents of that State has been or is threat-  
 21 ened or adversely affected by the engagement of  
 22 a business entity in a practice that is prohibited  
 23 under this subtitle, the State or the State or  
 24 local law enforcement agency on behalf of the  
 25 residents of the agency’s jurisdiction, may bring

1 a civil action on behalf of the residents of the  
2 State or jurisdiction in a district court of the  
3 United States of appropriate jurisdiction or any  
4 other court of competent jurisdiction, including  
5 a State court, to—

6 (i) enjoin that practice;

7 (ii) enforce compliance with this sub-  
8 title; or

9 (iii) obtain civil penalties of not more  
10 than \$500 per day per individual whose  
11 sensitive personally identifiable information  
12 was, or is reasonably believed to have been,  
13 accessed or acquired by an unauthorized  
14 person, up to a maximum of \$20,000,000  
15 per violation, unless such conduct is found  
16 to be willful or intentional.

17 (B) PRESUMPTION.—A violation of section  
18 212(a)(2) shall be presumed to be willful or in-  
19 tentional.

20 (2) CONSIDERATIONS.—In determining the  
21 amount of a civil penalty under this subsection, the  
22 court shall take into account—

23 (A) the degree of culpability of the busi-  
24 ness entity;

1 (B) any prior violations of this subtitle by  
2 the business entity;

3 (C) the ability of the business entity to pay  
4 a civil penalty;

5 (D) the effect on the ability of the business  
6 entity to continue to do business;

7 (E) the number of individuals whose per-  
8 sonally identifiable information was com-  
9 promised by the breach;

10 (F) the relative cost of compliance with  
11 this subtitle; and

12 (G) such other matters as justice may re-  
13 quire.

14 (3) NOTICE.—

15 (A) IN GENERAL.—Before filing an action  
16 under paragraph (1), the attorney general of  
17 the State involved shall provide to the Attorney  
18 General of the United States—

19 (i) written notice of the action; and

20 (ii) a copy of the complaint for the ac-  
21 tion.

22 (B) EXEMPTION.—

23 (i) IN GENERAL.—Subparagraph (A)  
24 shall not apply with respect to the filing of  
25 an action by an attorney general of a State

1 under this subtitle, if the State attorney  
2 general determines that it is not feasible to  
3 provide the notice described in such sub-  
4 paragraph before the filing of the action.

5 (ii) NOTIFICATION.—In an action de-  
6 scribed in clause (i), the attorney general  
7 of a State shall provide notice and a copy  
8 of the complaint to the Attorney General  
9 at the time the State attorney general files  
10 the action.

11 (b) FEDERAL PROCEEDINGS.—Upon receiving notice  
12 under subsection (a)(2), the Attorney General shall have  
13 the right to—

14 (1) move to stay the action, pending the final  
15 disposition of a pending Federal proceeding or ac-  
16 tion;

17 (2) initiate an action in the appropriate United  
18 States district court under section 217 and move to  
19 consolidate all pending actions, including State ac-  
20 tions, in such court;

21 (3) intervene in an action brought under sub-  
22 section (a)(2); and

23 (4) file petitions for appeal.

24 (c) PENDING PROCEEDINGS.—If the Attorney Gen-  
25 eral has instituted a proceeding or action for a violation



1 of this subtitle or any regulations thereunder, no attorney  
 2 general of a State may, during the pendency of such pro-  
 3 ceeding or action, bring an action under this subtitle  
 4 against any defendant named in such criminal proceeding  
 5 or civil action for any violation that is alleged in that pro-  
 6 ceeding or action.

7 (d) CONSTRUCTION.—For purposes of bringing any  
 8 civil action under subsection (a), nothing in this subtitle  
 9 regarding notification shall be construed to prevent an at-  
 10 torney general of a State from exercising the powers con-  
 11 ferred on such attorney general by the laws of that State  
 12 to—

- 13 (1) conduct investigations;
- 14 (2) administer oaths or affirmations; or
- 15 (3) compel the attendance of witnesses or the
- 16 production of documentary and other evidence.

17 (e) VENUE; SERVICE OF PROCESS.—

18 (1) VENUE.—Any action brought under sub-  
 19 section (a) may be brought in—

20 (A) the district court of the United States  
 21 that meets applicable requirements relating to  
 22 venue under section 1391 of title 28, United  
 23 States Code; or

24 (B) another court of competent jurisdic-  
 25 tion.

1           (2) SERVICE OF PROCESS.—In an action  
2       brought under subsection (a), process may be served  
3       in any district in which the defendant—

4                       (A) is an inhabitant; or

5                       (B) may be found.

6 **SEC. 220. SUPPLEMENTAL ENFORCEMENT BY INDIVIDUALS.**

7       (a) IN GENERAL.—Any person aggrieved by a viola-  
8       tion of the provisions of section 211, 213, 214, 215, or  
9       216 by a business entity may bring a civil action in a court  
10      of appropriate jurisdiction to recover for personal injuries  
11      sustained as a result of the violation.

12      (b) REMEDIES IN A CITIZEN SUIT.—

13           (1) DAMAGES.—Any individual harmed by a  
14       failure of a business entity to comply with the provi-  
15       sions of section 211, 213, 214, 215, or 216, shall be  
16       able to collect damages of not more than \$500 per  
17       day per individual whose sensitive personally identi-  
18       fiable information was, or is reasonably believed to  
19       have been, accessed or acquired by an unauthorized  
20       person, up to a maximum of \$20,000,000 per viola-  
21       tion.

22           (2) PUNITIVE DAMAGES.—A business entity  
23       may be liable for punitive damages if it—

1 (A) intentionally or willfully violates the  
2 provisions of section 211, 213, 214, 215, or  
3 216; or

4 (B) failed to comply with the requirements  
5 of subsections (a) through (d) of section 202.

6 (3) **EQUITABLE RELIEF.**—A business entity  
7 that violates the provisions of section 211, 213, 214,  
8 215, or 216 may be enjoined to provide required  
9 remedies under section 215 by a court of competent  
10 jurisdiction.

11 (4) **OTHER RIGHTS AND REMEDIES.**—The  
12 rights and remedies available under this subsection  
13 are cumulative and shall not affect any other rights  
14 and remedies available under law.

15 (c) **ACCESS TO JUSTICE.**—The rights and remedies  
16 afforded by this section shall not be abridged or precluded  
17 by any predispute arbitration agreement, and any claims  
18 under this section that arise from the same security  
19 breach are presumed to meet the commonality require-  
20 ment under rule 23(a)(2) of the Federal Rules of Civil  
21 Procedure.

22 **SEC. 221. RELATION TO OTHER LAWS.**

23 (a) **IN GENERAL.**—The provisions of this subtitle  
24 shall supersede any other provision of Federal law or any  
25 provision of law of any State relating to notification by

1 a business entity engaged in interstate commerce or an  
2 agency of a security breach, except as provided in section  
3 214(c).

4 (b) RULE OF CONSTRUCTION.—Nothing in this sub-  
5 title shall be construed to exempt any entity from liability  
6 under common law, including through the operation of or-  
7 dinary preemption principles, for damages caused by the  
8 failure to notify an individual following a security breach.

9 (c) PRESUMPTION OF PER SE NEGLIGENCE.—If a  
10 business entity fails to comply with the requirements in  
11 section 211, 212, 213, 214, 215, or 216, there shall be  
12 a presumption that the entity was per se negligent.

13 **SEC. 222. AUTHORIZATION OF APPROPRIATIONS.**

14 There are authorized to be appropriated such sums  
15 as may be necessary to cover the costs incurred by the  
16 United States Secret Service to carry out investigations  
17 and risk assessments of security breaches as required  
18 under this subtitle.

19 **SEC. 223. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

20 The United States Secret Service and the Federal  
21 Bureau of Investigation shall report to Congress not later  
22 than 18 months after the date of enactment of this Act,  
23 and upon the request by Congress thereafter, on—

24 (1) the number and nature of the security  
25 breaches described in the notices filed by those busi-

ness entities invoking the risk assessment exemption under section 212(b) and the response of the United States Secret Service and the Federal Bureau of Investigation to such notices; and

(2) the number and nature of security breaches subject to the national security and law enforcement exemptions under section 212(a), provided that such report may not disclose the contents of any risk assessment provided to the United States Secret Service and the Federal Bureau of Investigation pursuant to this subtitle.

## **Subtitle C—Post-Breach Technical Information Clearinghouse**

### **SEC. 230. CLEARINGHOUSE INFORMATION COLLECTION, MAINTENANCE, AND ACCESS.**

(a) IN GENERAL.—The Attorney General shall maintain a clearinghouse of technical information concerning system vulnerabilities identified in the wake of security breaches, which shall—

(1) contain information disclosed by agencies or business entities under subsection (b); and

(2) be accessible to certified entities under subsection (c).

(b) POST-BREACH TECHNICAL NOTIFICATION.—In any instance where an agency or business entity is re-

1 quired to notify the United States Secret Service and the  
2 Federal Bureau of Investigation under section 217, the  
3 agency or business entity shall also provide the Attorney  
4 General with technical information concerning the nature  
5 of the security breach, including—

6           (1) technical information regarding any system  
7       vulnerabilities of the agency or business entity re-  
8       vealed by or identified as a consequence of the secu-  
9       rity breach;

10           (2) technical information regarding any system  
11       vulnerabilities of the agency or business entity actu-  
12       ally exploited during the security breach; and

13           (3) any other technical information concerning  
14       the nature of the security breach deemed appro-  
15       priate for collection by the Attorney General in fur-  
16       therance of this subtitle.

17       (c) ACCESS TO CLEARINGHOUSE.—Any entity cer-  
18       tified under subsection (d) may review information main-  
19       tained by the technical information clearinghouse for the  
20       purpose of preventing security breaches that threaten the  
21       security of sensitive personally identifiable information.

22       (d) CERTIFICATION FOR ACCESS.—The Attorney  
23       General shall issue and revoke certifications to agencies  
24       and business entities wishing to review information main-  
25       tained by the technical information clearinghouse and

1 shall establish conditions for obtaining and maintaining  
 2 such certifications, including agreement that any informa-  
 3 tion obtained directly or derived indirectly from the review  
 4 of information maintained by the technical information  
 5 clearinghouse—

6 (1) shall only be used to improve the security  
 7 and reduce the vulnerability of networks that use  
 8 personally identifiable information;

9 (2) may not be used for any competitive com-  
 10 mercial purpose; and

11 (3) may not be shared with any third party, in-  
 12 cluding other parties certified for access to the infor-  
 13 mation clearinghouse, without the express written  
 14 consent of the Attorney General.

15 (e) RULEMAKING.—In consultation with the private  
 16 sector, appropriate representatives of State and local gov-  
 17 ernments, and other appropriate Federal agencies, the At-  
 18 torney General shall promulgate any regulations pursuant  
 19 to section 553 of title 5, United States Code, necessary  
 20 to carry out the provisions of this section.

21 **SEC. 231. PROTECTIONS FOR CLEARINGHOUSE PARTICI-**  
 22 **PANTS.**

23 (a) PROTECTION OF PROPRIETARY INFORMATION.—  
 24 To the extent feasible, the Attorney General shall ensure  
 25 that any technical information disclosed to the Attorney

1 General under this subtitle shall be stored in a format de-  
2 signed to protect proprietary business information from  
3 inadvertent disclosure.

4 (b) ANONYMOUS DATA RELEASE.—To the extent fea-  
5 sible, the Attorney General shall ensure that all informa-  
6 tion stored in the technical information clearinghouse and  
7 accessed by certified parties is presented in a form that  
8 minimizes the potential for such information to be traced  
9 to a particular network, company, or security breach inci-  
10 dent.

11 (c) PROTECTION FROM PUBLIC DISCLOSURE.—Ex-  
12 cept as otherwise provided in this subtitle—

13 (1) security and vulnerability information col-  
14 lected under this section and provided to the Federal  
15 Government, including aggregated analysis and data,  
16 shall be exempt from disclosure under section  
17 552(b)(3) of title 5, United States Code; and

18 (2) under section 230(e), security and vulner-  
19 ability-related information provided to the Federal  
20 Government under this section, including aggregated  
21 analysis and data, shall be protected from public dis-  
22 closure, except that this paragraph—

23 (A) does not prohibit the sharing of such  
24 information, as the Attorney General deter-  
25 mines to be appropriate, in order to mitigate



1 cybersecurity threats or further the official  
 2 functions of a government agency; and

3 (B) does not authorized such information  
 4 to be withheld from a committee of Congress  
 5 authorized to request the information.

6 (d) PROTECTION OF CLASSIFIED INFORMATION.—  
 7 Nothing in this subtitle permits the unauthorized dislo-  
 8 sure of classified information.

9 **SEC. 232. EFFECTIVE DATE.**

10 This subtitle shall take effect on the expiration of the  
 11 date which is 90 days after the date of enactment of this  
 12 Act.

13 **TITLE III—ACCESS TO AND USE**  
 14 **OF COMMERCIAL DATA**

15 **SEC. 301. GENERAL SERVICES ADMINISTRATION REVIEW**  
 16 **OF CONTRACTS.**

17 (a) IN GENERAL.—In considering contract awards  
 18 totaling more than \$500,000 and entered into after the  
 19 date of enactment of this Act with data brokers, the Ad-  
 20 ministrator of the General Services Administration shall  
 21 evaluate—

22 (1) the data privacy and security program of a  
 23 data broker to ensure the privacy and security of  
 24 data containing personally identifiable information,  
 25 including whether such program adequately address-

1 es privacy and security threats created by malicious  
2 software or code, or the use of peer-to-peer file shar-  
3 ing software;

4 (2) the compliance of a data broker with such  
5 program;

6 (3) the extent to which the databases and sys-  
7 tems containing personally identifiable information  
8 of a data broker have been compromised by security  
9 breaches; and

10 (4) the response by a data broker to such  
11 breaches, including the efforts by such data broker  
12 to mitigate the impact of such security breaches.

13 (b) COMPLIANCE SAFE HARBOR.—The data privacy  
14 and security program of a data broker shall be deemed  
15 sufficient for the purposes of subsection (a), if the data  
16 broker complies with or provides protection equal to indus-  
17 try standards, as identified by the Federal Trade Commis-  
18 sion, that are applicable to the type of personally identifi-  
19 able information involved in the ordinary course of busi-  
20 ness of such data broker.

21 (c) PENALTIES.—In awarding contracts with data  
22 brokers for products or services related to access, use,  
23 compilation, distribution, processing, analyzing, or evalu-  
24 ating personally identifiable information, the Adminis-  
25 trator of the General Services Administration shall—

1 (1) include monetary or other penalties—

2 (A) for failure to comply with subtitles A  
3 and B of title III; or

4 (B) if a contractor knows or has reason to  
5 know that the personally identifiable informa-  
6 tion being provided is inaccurate, and provides  
7 such inaccurate information; and

8 (2) require a data broker that engages service  
9 providers not subject to subtitle A of title III for re-  
10 sponsibilities related to sensitive personally identifi-  
11 able information to—

12 (A) exercise appropriate due diligence in  
13 selecting those service providers for responsibil-  
14 ities related to personally identifiable informa-  
15 tion;

16 (B) take reasonable steps to select and re-  
17 tain service providers that are capable of main-  
18 taining appropriate safeguards for the security,  
19 privacy, and integrity of the personally identifi-  
20 able information at issue; and

21 (C) require such service providers, by con-  
22 tract, to implement and maintain appropriate  
23 measures designed to meet the objectives and  
24 requirements in title III.

1 (d) LIMITATION.—The penalties under subsection (c)  
 2 shall not apply to a data broker providing information that  
 3 is accurately and completely recorded from a public record  
 4 source or licensor.

5 **SEC. 302. REQUIREMENT TO AUDIT INFORMATION SECU-**  
 6 **RITY PRACTICES OF CONTRACTORS AND**  
 7 **THIRD PARTY BUSINESS ENTITIES.**

8 Section 3544(b) of title 44, United States Code, is  
 9 amended—

10 (1) in paragraph (7)(C)(iii), by striking “and”  
 11 after the semicolon;

12 (2) in paragraph (8), by striking the period and  
 13 inserting “; and”; and

14 (3) by adding at the end the following:

15 “(9) procedures for evaluating and auditing the  
 16 information security practices of contractors or third  
 17 party business entities supporting the information  
 18 systems or operations of the agency involving per-  
 19 sonally identifiable information (as that term is de-  
 20 fined in section 3 of the Personal Data Protection  
 21 and Breach Accountability Act of 2011) and ensur-  
 22 ing remedial action to address any significant defi-  
 23 ciencies.”.

1 **SEC. 303. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**  
 2 **USE OF COMMERCIAL INFORMATION SERV-**  
 3 **ICES CONTAINING PERSONALLY IDENTIFI-**  
 4 **ABLE INFORMATION.**

5 (a) IN GENERAL.—Section 208(b)(1) of the E-Gov-  
 6 ernment Act of 2002 (44 U.S.C. 3501 note) is amended—

7 (1) in subparagraph (A)(i), by striking “or”;

8 (2) in subparagraph (A)(ii), by striking the pe-  
 9 riod and inserting “; or”; and

10 (3) by inserting after clause (ii) the following:

11 “(iii) purchasing or subscribing for a  
 12 fee to personally identifiable information  
 13 from a data broker (as such terms are de-  
 14 fined in section 3 of the Personal Data  
 15 Protection and Breach Accountability Act  
 16 of 2011).”.

17 (b) LIMITATION.—Notwithstanding any other provi-  
 18 sion of law, commencing 1 year after the date of enact-  
 19 ment of this Act, no Federal agency may enter into a con-  
 20 tract with a data broker to access for a fee any database  
 21 consisting primarily of personally identifiable information  
 22 concerning United States persons (other than news report-  
 23 ing or telephone directories) unless the head of such de-  
 24 partment or agency—

25 (1) completes a privacy impact assessment  
 26 under section 208 of the E-Government Act of 2002

1 (44 U.S.C. 3501 note), which shall subject to the  
2 provision in that Act pertaining to sensitive informa-  
3 tion, include a description of—

4 (A) such database;

5 (B) the name of the data broker from  
6 whom it is obtained; and

7 (C) the amount of the contract for use;

8 (2) adopts regulations that specify—

9 (A) the personnel permitted to access, ana-  
10 lyze, or otherwise use such databases;

11 (B) standards governing the access, anal-  
12 ysis, or use of such databases;

13 (C) any standards used to ensure that the  
14 personally identifiable information accessed,  
15 analyzed, or used is the minimum necessary to  
16 accomplish the intended legitimate purpose of  
17 the Federal agency;

18 (D) standards limiting the retention and  
19 redisclosure of personally identifiable informa-  
20 tion obtained from such databases;

21 (E) procedures ensuring that such data  
22 meet standards of accuracy, relevance, com-  
23 pleteness, and timeliness;

1 (F) the auditing and security measures to  
2 protect against unauthorized access, analysis,  
3 use, or modification of data in such databases;

4 (G) applicable mechanisms by which indi-  
5 viduals may secure timely redress for any ad-  
6 verse consequences wrongly incurred due to the  
7 access, analysis, or use of such databases;

8 (H) mechanisms, if any, for the enforce-  
9 ment and independent oversight of existing or  
10 planned procedures, policies, or guidelines; and

11 (I) an outline of enforcement mechanisms  
12 for accountability to protect individuals and the  
13 public against unlawful or illegitimate access or  
14 use of databases; and

15 (3) incorporates into the contract or other  
16 agreement totaling more than \$500,000, provi-  
17 sions—

18 (A) providing for penalties—

19 (i) for failure to comply with title III  
20 of this Act; or

21 (ii) if the entity knows or has reason  
22 to know that the personally identifiable in-  
23 formation being provided to the Federal  
24 department or agency is inaccurate, and  
25 provides such inaccurate information; and

(B) requiring a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(i) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(ii) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(iii) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(c) LIMITATION ON PENALTIES.—The penalties under subsection (b)(3)(A) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source.

(d) STUDY OF GOVERNMENT USE.—

(1) SCOPE OF STUDY.—Not later than 180 days after the date of enactment of this Act, the



1 Comptroller General of the United States shall con-  
2 duct a study and audit and prepare a report on Fed-  
3 eral agency actions to address the recommendations  
4 in the Government Accountability Office's April  
5 2006 report on agency adherence to key privacy  
6 principles in using data brokers or commercial data-  
7 bases containing personally identifiable information.

8 (2) REPORT.—A copy of the report required  
9 under paragraph (1) shall be submitted to Congress.

10 **SEC. 304. FBI REPORT ON REPORTED BREACHES AND COM-**  
11 **PLIANCE.**

12 (a) IN GENERAL.—Not later than 1 year after the  
13 date of enactment of this Act, and each year thereafter,  
14 the Federal Bureau of Investigation, in coordination with  
15 the Secret Service, shall submit to the Committee on the  
16 Judiciary of the Senate and the Committee on the Judici-  
17 ary of the House of Representatives a report regarding  
18 any reported breaches at agencies or business entities dur-  
19 ing the preceding year.

20 (b) REPORT CONTENT.—Such reporting shall in-  
21 clude—

22 (1) the total instances of breaches of security in  
23 the previous year;

24 (2) the percentage of breaches described in sub-  
25 section (a) that occurred at an agency or business

1       entity that did not comply with the personal data  
2       privacy and security program under section 202; and  
3       (3) recommendations, if any, for modifying or  
4       amending this Act to increase its effectiveness.

5   **SEC. 305. DEPARTMENT OF JUSTICE REPORT ON ENFORCE-**  
6                   **MENT ACTIONS.**

7       (a) IN GENERAL.—Not later than 1 year after the  
8       date of enactment of this Act, and each year thereafter,  
9       the Attorney General shall submit to Congress a report  
10      on the enforcement actions taken in the previous year in  
11      cases of violations of any sections of this Act.

12      (b) REPORT CONTENT.—The report required under  
13      subsection (a) shall include—

14           (1) statistics on Federal enforcement actions,  
15           State attorneys general enforcement actions, and  
16           private enforcement actions related to the provisions  
17           of this Act; and

18           (2) recommendations, if any, for modifying of  
19           amending this Act to increase the effectiveness of  
20           such enforcement actions.

21   **SEC. 306. DEPARTMENT OF JUSTICE REPORT ON ENFORCE-**  
22                   **MENT ACTIONS.**

23      Section 529 of title 28, United States Code, is  
24      amended by adding at the end the following:

1       “(c) Not later than 1 year after the date of enactment  
2 of the Personal Data Protection and Breach Account-  
3 ability Act of 2011, and every fiscal year thereafter, the  
4 Attorney General shall submit to Congress a report on the  
5 efforts of the Federal Government to enforce the Personal  
6 Data Protection and Breach Accountability Act of 2011  
7 that shall include a description of the best practices for  
8 enforcement of such Act.”.

9   **SEC. 307. FBI REPORT ON NOTIFICATION EFFECTIVENESS.**

10       (a) IN GENERAL.—Not later than 1 year after the  
11 date of enactment of this Act, and each year thereafter,  
12 the Federal Bureau of Investigation, in coordination with  
13 the Secret Service, shall submit to the Committee on the  
14 Judiciary of the Senate and the Committee on the Judici-  
15 ary of the House of Representatives a report regarding  
16 the effectiveness of post-breach notification practices by  
17 agencies and business entities.

18       (b) REPORT CONTENT.—The report required under  
19 subsection (a) shall include—

20               (1) in each instance of a breach of security, the  
21 amount of time between the instance of the breach  
22 and the discovery of the breach by the affected busi-  
23 ness entity;

24               (2) in each instance of a breach of security, the  
25 amount of time between the discovery of the breach

1 by the affected business entity and the notification  
2 to the FBI and Secret Service; and

3 (3) in each instance of a breach of security, the  
4 amount of time between the discovery of the breach  
5 by the affected business entity and the notification  
6 to individuals whose sensitive personally identifiable  
7 information was compromised.

8 **TITLE IV—COMPLIANCE WITH**  
9 **STATUTORY PAY-AS-YOU-GO ACT**

10 **SEC. 401. BUDGET COMPLIANCE.**

11 The budgetary effects of this Act, for the purpose of  
12 complying with the Statutory Pay-As-You-Go Act of 2010,  
13 shall be determined by reference to the latest statement  
14 titled “Budgetary Effects of PAYGO Legislation” for this  
15 Act, submitted for printing in the Congressional Record  
16 by the Chairman of the Senate Budget Committee, pro-  
17 vided that such statement has been submitted prior to the  
18 vote on passage.

○